Japanese Patent Laid-open No. 2003-283555 A
Publication date : October 3, 2003
Applicant : NIPPON TELEGRAPH AND TELEPHONE CORPORATION
Title : DISTRIBUTED DENIAL OF SERVICE ATTACK PREVENTING METHOD AND GATE DEVICE, COMMUNICATION DEVICE, AND PROGRAM

[Scope of Claims for Patent]

[Claim 1]

A distributed denial of service attack preventing method, wherein

in a network system including a network consisting of a plurality of communication devices connected with each other in a mesh, a computer and a LAN to be protected, and a gate device which is inserted between the LAN and the network,

the gate device, when a suspicious offensive traffic is detected from an input communication traffic, executes processing of calculating, based on a transmission band limit value of the suspicious offensive traffic in the corresponding gate device and the number of communication devices in one-level-upstream of the corresponding gate device, a transmission band limit value of the suspicious offensive traffic to be notified to the upstream communication devices, and transmitting a calculation result to the upstream communication devices,

the communication device executes processing of limiting a transmission band of the suspicious offensive traffic to the transmission band limit value received from the downstream gate device or communication device, calculating, based on the received transmission band limit value and the number of communication devices in one-level-upstream of the corresponding communication device, a transmission band limit value of the suspicious offensive

traffic to be notified to the upstream communication devices, and transmitting the calculation result to the upstream communication devices,

the communication device further executes recursive processing of limiting the transmission band of a suspicious offensive packet, and transmitting the transmission band limit value of the suspicious offensive traffic until reaching the uppermost communication device serving as a sending end of the suspicious offensive packet,

the gate device executes processing of transmitting a query of an average input transmission band of the suspicious offensive traffic to the upstream communication device,

the upstream communication device executes processing of receiving the query of the average input transmission band of the suspicious offensive traffic from the downstream gate device or communication device, and transmitting an average input transmission band value of the suspicious offensive traffic in the corresponding communication device to the downstream gate device or communication device,

the gate device executes processing of calculating, based on a transmission band limit adjusted value of the suspicious offensive traffic in the corresponding gate device and the average input transmission band value of the suspicious offensive traffic received from the upstream communication device, a transmission band limit adjusted value of the suspicious offensive traffic to be notified to the upstream communication device, and transmitting the calculation result to the upstream communication device,

the communication device executes processing of limiting the transmission band of the suspicious offensive traffic to the transmission band limit adjusted value

received from the downstream gate device or communication device, and transmitting a query of the average input transmission band of the suspicious offensive traffic to the upstream communication device, and further executes processing of calculating, based on the transmission band limit adjusted value received from the downstream communication device and the average input transmission band value of the suspicious offensive traffic received from the upstream communication device, a transmission band limit adjusted value of the suspicious offensive traffic to be notified to the upstream communication device, and transmitting the calculation result to the upstream communication device, and

the communication device further executes recursive processing of limiting the transmission band of the suspicious offensive packet to the transmission band limit adjusted value, and transmitting the transmission band limit adjusted value of the suspicious offensive traffic until reaching the uppermost communication device serving as the sending end of the suspicious offensive packet.

[Brief Description of Drawings]

[Fig. 1] A structural view of a network to which an embodiment of the present invention can be applied.

[Fig. 2] An example of setting conditions for detecting suspicious attacks according to the embodiment.

[Fig. 3] An example of setting conditions for detecting illegal traffics according to the embodiment.

[Fig. 4] A model of band control included in a gate device 2001 and communication devices 2002 to 2006 according to the embodiment.

[Fig. 5] A classification algorism in a filter 2021 according to the embodiment.

[Fig. 6] A flowchart of an operation of the gate device 2001 according to the embodiment when a suspicious offensive packet is detected.

[Fig. 7] An example of calculation of a transmission band limit value in the configuration shown in Fig. of the embodiment.

[Fig. 8] A flowchart of an operation of the communication devices 2002 and 2003 according to the embodiment when receiving a transmission band limiting instruction.

[Fig. 9] A flowchart of an operation of the gate device 2001 and the communication devices 2002 to 2006 according to the embodiment when an illegal traffic is detected.

[Fig. 10] An example of calculation of a transmission band limit adjusted value in the configuration shown in Fig. of the embodiment.

[Fig. 11] A flowchart of an operation of adjusting the transmission band limit value performed by the gate device 2001 and the communication devices 2002 to 2006 according to the embodiment.

Fig. 1

2007, 2008
TERMINAL DEVICE
DDos ATTACKER

2009, 2010
TERMINAL DEVICE
LEGITIMATE USER

2002 to 2006 COMMUNICATION DEVICE (ROUTER)

NETWORK
2001 GATE DEVICE (GATEWAY)

2000

SERVER

DDos ATTACKED PERSON

Fig. 2

NUMBER

DETECTED ATTRIBUTE

DETECTED THRESHOLD

DETECTION INTERVAL

10 SECONDS

20 SECONDS

Fig. 3

NUMBER	CONDITIONS OF ILLEGAL TRAFFIC
	PACKETS OF T1 Kbps OR MORE ARE SUCCESSIVELY TRANSMITTED FOR S1 SECOND OR LONGER.
	ICMP/Echo Reply PACKETS OF T2 Kbps OR MORE ARE SUCCESSIVELY TRANSMITTED FOR S2 SECONDS OR LONGER.
	FRAGMENT PACKETS OF T3 Kbps OR MORE ARE SUCCESSIVELY TRANSMITTED FOR S3 SECONDS OR LONGER.

Fig. 4

INPUT

2021 FILTER

2022 NORMAL CLASS

2023 NORMAL QUEUE

OUTPUT

2026 SUSPICIOUS CLASS

2027 SUSPICIOUS QUEUE

2024 ILLEGAL CLASS

2025 ILLEGAL QUEUE

Fig. 5

INPUT

S3003 DOES INPUT PACKET COINCIDE WITH ILLEGAL SIGNATURE?

S3004 PUT IN ILLEGAL QUEUE

S3005 DOES INPUT PACKET COINCIDE WITH SUSPICIOUS SIGNATURE?

S3006 PUT IN SUSPICIOUS QUEUE

S3007 PUT IN NORMAL QUEUE

OUTPUT

Fig. 6

START

S3011 DETECT SUSPICIOUS OFFENSIVE TRAFFIC

S3012 CREATE SUSPICIOUS SIGNATURE

S3013 REGISTER SUSPICIOUS SIGNATURE IN FILTER AND CREATE SUSPICIOUS QUEUE

S3014 SEND TRANSMISSION BAND LIMITING INSTRUCTION TO UPSTREAM COMMUNICATION DEVICE

Fig. 7

2007, 2008

TERMINAL DEVICE

DDos ATTACKER

2009, 2010

TERMINAL DEVICE

LEGITIMATE USER

2002 to 2006 COMMUNICATION DEVICE (ROUTER)

2001 GATE DEVICE (GATEWAY)

2000

SERVER

DDos ATTACKED PERSON

Fig. 8

START

S3021 RECEIVE TRANSMISSION BAND LIMITING INSTRUCTION FROM DOWNSTREAM COMMUNICATION DEVICE

S3022 REGISTER SUSPICIOUS SIGNATURE IN FILTER AND CREATE SUSPICIOUS QUEUE

S3033 SEND TRANSMISSION BAND LIMITING INSTRUCTION TO UPSTREAM COMMUNICATION DEVICE

Fig. 9

START

S3031 DETECT ILLEGAL TRAFFIC

S3032 CREATE ILLEGAL SIGNATURE

S3033 REGISTER ILLEGAL SIGNATURE IN FILTER

Fig. 10

2007, 2008

TERMINAL DEVICE

DDos ATTACKER

2009, 2010

TERMINAL DEVICE

LEGITIMATE USER

OFFENSIVE PACKET

SUSPICIOUS OFFENSIVE PACKET

2002 to 2006 COMMUNICATION DEVICE (ROUTER)

2001 GATE DEVICE (GATEWAY)

2000

SERVER

DDos ATTACKED PERSON

Fig. 11

COMMUNICATION DEVICE (ROUTER)

START

S3061 RECEIVE QUERY OF AVERAGE INPUT TRANSMISSION BAND FROM DOWNSTREAM COMMUNICATION DEVICE

S3062 TRANSMIT AVERAGE INPUT TRANSMISSION BAND VALUE TO DOWNSTREAM COMMUNICATION DEVICE

S3063 RECEIVE TRANSMISSION BAND ADJUSTING INSTRUCTION FROM DOWNSTREAM COMMUNICATION DEVICE

S3064 CHANGE TRANSMISSION BAND LIMIT VALUE TO TRANSMISSION BAND LIMIT ADJUSTED VALUE

END

COMMUNICATION DEVICE (ROUTER)

START

S3051 RECEIVE QUERY OF AVERAGE INPUT TRANSMISSION BAND FROM DOWNSTREAM COMMUNICATION DEVICE

S3052 TRANSMIT AVERAGE INPUT TRANSMISSION BAND VALUE TO DOWNSTREAM COMMUNICATION DEVICE

S3053 RECEIVE TRANSMISSION BAND ADJUSTING INSTRUCTION FROM DOWNSTREAM COMMUNICATION DEVICE

S3054 CHANGE TRANSMISSION BAND LIMIT VALUE TO TRANSMISSION BAND LIMIT ADJUSTED VALUE

S3055 TRANSMIT QUERY OF AVERAGE INPUT TRANSMISSION BAND TO ALL UPSTREAM COMMUNICATION DEVICES

S3056 RECEIVE AVERAGE INPUT TRANSMISSION BAND VALUE FROM ALL UPSTREAM COMMUNICATION DEVICES

S3057 TRANSMIT TRANSMISSION BAND ADJUSTING INSTRUCTION TO ALL UPSTREAM COMMUNICATION DEVICES

END

GATE DEVICE (GATEWAY)

START

S3041 TRANSMIT QUERY OF AVERAGE INPUT TRANSMISSION BAND TO ALL UPSTREAM COMMUNICATION DEVICES

S3042 RECEIVE AVERAGE INPUT TRANSMISSION BAND VALUE FROM ALL UPSTREAM COMMUNICATION DEVICES

S3043 SEND TRANSMISSION BAND ADJUSTING INSTRUCTION TO ALL UPSTREAM COMMUNICATION DEVICES

S3044 DETECT TRIGGER

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－283555
（P2003－283555A）
(43)公開日　平成15年10月３日(2003.10.3)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　12/56	２００	Ｈ０４Ｌ　12/56	２００Ｚ	５Ｋ０３０
12/46		12/46	Ｅ	５Ｋ０３３

審査請求　有　　請求項の数13　ＯＬ　（全 25 頁）

(21)出願番号　特願2002－81905(P2002－81905)

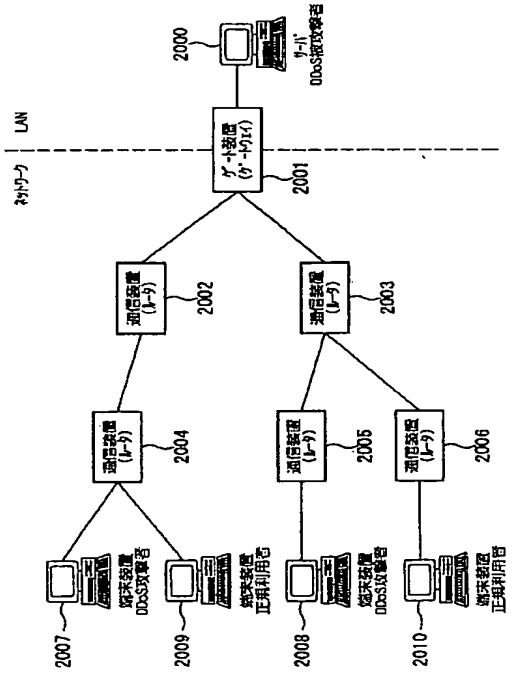
(22)出願日　平成14年３月22日(2002.3.22)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　柏　大
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　エリック・チェン
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100064908
弁理士　志賀　正武　（外２名）

最終頁に続く

(54)【発明の名称】　分散型サービス不能攻撃防止方法及びゲート装置、通信装置ならびにプログラム

(57)【要約】
【課題】　正規利用者の通信トラヒックを確保しながら、分散型サービス不能攻撃（ＤＤｏＳ攻撃）の攻撃トラヒックの伝送帯域を制限することを可能とする。
【解決手段】　ゲート装置２００１は、ＤＤｏＳ攻撃の攻撃容疑パケットを検出すると、上流の通信装置２００２、２００３に攻撃容疑パケットの伝送帯域制限値を通知する。上流の通信装置２００２、２００３は、攻撃容疑パケットの伝送帯域を受信した伝送帯域制限値に制限しながら、さらに上流の通信装置に伝送帯域制限値の通知を最上流まで繰り返し、各通信装置が攻撃容疑パケットの伝送帯域を制限する。一定時間経過後、ゲート装置２００１は通信装置２００２、２００３から攻撃容疑パケットの平均入力伝送帯域値を受信し、この平均入力伝送帯域の比率により伝送帯域制限調整値を算出し、各通信装置は再帰的に最上流の通信装置まで伝送帯域制限調整値を通知し、伝送帯域制限を調整する。



1

【特許請求の範囲】

【請求項１】　複数の通信装置を網目状に接続してなるネットワークと、防御対象であるコンピュータおよびＬＡＮと、前記ＬＡＮおよびネットワークの間に介挿されたゲート装置とを有するネットワークシステムにおいて、

前記ゲート装置は、

入力される通信トラヒックから攻撃容疑トラヒックを検出した場合に、当該ゲート装置における前記攻撃容疑トラヒックの伝送帯域制限値と、当該ゲート装置の１つ上流にある通信装置数とを基に、上流の前記通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限値を算出して上流の前記通信装置へ送信する処理を行い、

前記通信装置は、

前記攻撃容疑トラヒックの伝送帯域を下流のゲート装置または通信装置から受信した前記伝送帯域制限値に制限すると共に、前記受信した伝送帯域制限値と、当該通信装置の１つ上流にある通信装置数とを基に、上流の前記通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限値を算出して上流の通信装置へ送信する処理を行い、

前記攻撃容疑パケット送出元の最上流の前記通信装置に達するまで再帰的に、前記攻撃容疑パケットの伝送帯域の制限と、前記攻撃容疑トラヒックの伝送帯域制限値送信との処理を行い、

前記ゲート装置は、

前記上流の通信装置へ前記攻撃容疑トラヒックの平均入力伝送帯域を問合せを送信する処理を行い、

前記上流の通信装置は、

前記下流のゲート装置または通信装置から前記攻撃容疑トラヒックの平均入力伝送帯域問合せを受信して、当該通信装置における前記攻撃容疑トラヒックの平均入力伝送帯域値を前記下流のゲート装置または通信装置へ送信する処理を行い、

前記ゲート装置は、

当該ゲート装置における前記攻撃容疑トラヒックの伝送帯域制限調整値と、前記上流の通信装置から受信した前記攻撃容疑トラヒックの平均入力伝送帯域値とを基に、上流の通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限調整値を算出して前記上流の通信装置へ送信する処理を行い、

前記通信装置は、

前記攻撃容疑トラヒックの伝送帯域を下流のゲート装置または通信装置から受信した前記伝送帯域制限調整値に制限すると共に、前記上流の通信装置へ前記攻撃容疑トラヒックの平均入力伝送帯域を問合せを送信する処理と、前記下流の通信装置から受信した伝送帯域制限調整値と、前記上流の通信装置から受信した前記攻撃容疑トラヒックの平均入力伝送帯域値とを基に、上流の通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限調整値を算出して前記上流の通信装置へ送信する処理とを行い、

2

前記攻撃容疑パケット送出元の最上流の前記通信装置に達するまで再帰的に、伝送帯域制限調整値に前記攻撃容疑パケットの伝送帯域の制限と共に、前記攻撃容疑トラヒックの伝送帯域制限調整値の送信との処理を行う、

ことを特徴とする分散型サービス不能攻撃防止方法。

【請求項２】　前記伝送帯域制限値は、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さをｄ、同一の深さｄにおいてゲート装置または通信装置を識別する番号をｉ、深さｄにあるｉで識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域制限値をＳｓ(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置数をnu(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置を識別するための番号をｋ、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にあるｋで識別される通信装置の攻撃容疑トラヒックの伝送帯域制限値をＳｓ(d+1, i, k)とすると、

【数１】

$$Ss_{(d+1,i,k)} = \frac{1}{nu_{(d,i)}} \quad Ss_{(d,i)}$$

により算出されることを特徴とする請求項１に記載の分散型サービス不能攻撃防止方法。

【請求項３】　前記伝送帯域制限調整値は、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さをｄ、同一の深さｄにおいてゲート装置または通信装置を識別する番号をｉ、深さｄにあるｉで識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域調整値をＳｓ’(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置数をnu(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置を識別するための番号をｋ、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にあるｋで識別される通信装置から通知された攻撃容疑トラヒックの平均入力伝送帯域値をＢ(d+1, i, k)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にあるｋで識別される通信装置の攻撃容疑トラヒックの伝送帯域制限調整値をＳｓ’(d+1, i, k)とすると、

【数２】

$$Ss'_{(d+1,i,k)} = \frac{B_{(d+1,i,k)}}{nu_{(d,i)} \sum_{l=1} B_{(d+1,i,l)}} \quad Ss'_{(d,i)}$$

により算出されることを特徴とする請求項１または請求

項２に記載の分散型サービス不能攻撃防止方法。

【請求項４】　複数の通信装置を網目状に接続してなるネットワークと、防御対象であるコンピュータおよびＬＡＮとの間に介挿されたゲート装置において、

入力される通信トラヒックをチェックし、分散型サービス不能攻撃の攻撃容疑トラヒックを検出するトラヒック監視手段と、

当該ゲート装置における前記攻撃容疑トラヒックの伝送帯域制限値と、当該ゲート装置の１つ上流にある通信装置数とを基に、上流の前記通信装置へ通知する前記トラヒック監視手段によって検出された攻撃容疑トラヒックの伝送帯域制限値を算出して上流の通信装置へ送信する帯域制限指示手段と、

前記上流の通信装置へ前記攻撃容疑トラヒックの平均入力伝送帯域を問い合わせる伝送帯域問合せ手段と、

前記上流の通信装置から前記攻撃容疑トラヒックの平均入力伝送帯域値を受信する伝送帯域値受信手段と、

当該ゲート装置における前記攻撃容疑トラヒックの伝送帯域制限調整値と、前記上流の通信装置から受信した前記攻撃容疑トラヒックの平均入力伝送帯域値とを基に、上流の通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限調整値を算出して前記上流の通信装置へ送信する帯域制限調整手段と、

を備えることを特徴とするゲート装置。

【請求項５】　前記帯域制限指示手段は、前記伝送帯域制限値を、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さをｄ、同一の深さｄにおいてゲート装置または通信装置を識別する番号をｉ、深さｄにあるｉで識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域制限値をＳｓ＊(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置数をnu(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置を識別するための番号をｋ、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にあるｋで識別される通信装置の攻撃容疑トラヒックの伝送帯域制限値をＳｓ(d+1, i, k)とすると、

【数３】

$$Ss_{(d+1,i,k)} = \frac{1}{nu_{(d,i)}} \quad Ss_{(d,i)}$$

により算出し、

前記帯域制限調整手段は、前記伝送帯域調整値を、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さをｄ、同一の深さｄにおいてゲート装置または通信装置を識別する番号をｉ、深さｄにあるｉで識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域調整値をＳｓ’(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置数をnu(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置を識別するための番号をｋ、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にあるｋで識別される通信装置から通知された攻撃容疑トラヒックの平均入力伝送帯域値をＢ(d+1, i, k)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にあるｋで識別される通信装置の攻撃容疑トラヒックの伝送帯域制限調整値をＳｓ’(d+1, i, k)とすると、

【数４】

$$Ss'_{(d+1,i,k)} = \frac{B_{(d+1,i,k)}}{\sum_{l=1}^{nu_{(d,i)}} B_{(d+1,i,l)}} \quad Ss'_{(d,i)}$$

により算出することを特徴とする請求項４に記載のゲート装置。

【請求項６】　防御対象であるコンピュータおよびＬＡＮを防御するゲート装置が接続されたネットワークのノードを構成する通信装置において、

下流のゲート装置あるいは通信装置から攻撃容疑トラヒックの伝送帯域制限値を受信し、前記攻撃容疑トラヒックの伝送帯域を前記伝送帯域制限値に制限する帯域制御手段と、

前記受信した伝送帯域制限値と、当該通信装置の１つ上流にある通信装置数とを基に、上流の前記通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限値を算出して上流の通信装置へ送信する帯域制限指示手段と、

前記下流のゲート装置あるいは通信装置から前記攻撃容疑トラヒックの平均入力伝送帯域問い合わせを受信し、当該通信装置における前記攻撃容疑トラヒックの平均入力伝送帯域値を前記下流のゲート装置あるいは通信装置へ送信する帯域通知手段と、

前記下流のゲート装置あるいは通信装置から攻撃容疑トラヒックの伝送帯域制限調整値を受信し、前記攻撃容疑トラヒックの伝送帯域を前記伝送帯域制限調整値に制限する帯域制御調整手段と、

前記上流の通信装置へ前記攻撃容疑トラヒックの平均入力伝送帯域を問い合わせる伝送帯域問合せ手段と、

前記上流の通信装置から前記攻撃容疑トラヒックの平均入力伝送帯域値を受信する伝送帯域値受信手段と、

前記上流の通信装置から受信した前記攻撃容疑トラヒックの平均入力伝送帯域値と前記受信した伝送帯域制限調

整値とを基に、上流の通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限調整値を算出して、前記上流の通信装置へ送信する帯域制限調整手段と、
を備えることを特徴とする通信装置。

【請求項７】　前記帯域制限指示手段は、前記伝送帯域制限値を、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さをｄ、同一の深さｄにおいてゲート装置または通信装置を識別する番号をｉ、深さｄにあるｉで識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域制限値をＳｓ(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置数をnu(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置を識別するための番号をｋ、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にあるｋで識別される通信装置の攻撃容疑トラヒックの伝送帯域制限値をＳｓ(d+1, i, k)とすると、

【数５】

$$Ss_{(d+1,i,k)} = \frac{1}{nu_{(d,i)}} \quad Ss_{(d,i)}$$

により算出し、
前記帯域制限調整手段は、前記伝送帯域調整値を、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さをｄ、同一の深さｄにおいてゲート装置または通信装置を識別する番号をｉ、深さｄにあるｉで識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域調整値をＳｓ’(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置数をnu(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置を識別するための番号をｋ、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にあるｋで識別される通信装置から通知された攻撃容疑トラヒックの平均入力伝送帯域値をＢ(d+1, i, k)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にあるｋで識別される通信装置の攻撃容疑トラヒックの伝送帯域制限調整値をＳｓ’(d+1, i, k)とすると、

【数６】

$$Ss'_{(d+1,i,k)} = \frac{B_{(d+1,i,k)}}{\sum_{l=1}^{nu_{(d,i)}} B_{(d+1,i,l)}} \quad Ss'_{(d,i)}$$

により算出することを特徴とする請求項６に記載の通信装置。

【請求項８】　複数の通信装置を網目状に接続してなるネットワークと、防御対象であるコンピュータおよびＬＡＮとの間に介挿されたゲート装置上で実行されるコンピュータプログラムであって、
入力される通信トラヒックをチェックし、分散型サービス不能攻撃の攻撃容疑トラヒックを検出した場合に、当該ゲート装置における前記攻撃容疑トラヒックの伝送帯域制限値と、当該ゲート装置の１つ上流にある通信装置数とを基に、上流の前記通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限値を算出して上流の通信装置へ送信するステップと、
前記上流の通信装置へ前記攻撃容疑トラヒックの平均入力伝送帯域を問合せを送信するステップと、
前記上流の通信装置から前記攻撃容疑トラヒックの平均入力伝送帯域値を受信するステップと、
当該ゲート装置における前記攻撃容疑トラヒックの伝送帯域制限調整値と、前記上流の通信装置から受信した前記攻撃容疑トラヒックの平均入力伝送帯域値とを基に、上流の前記通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限調整値を算出して前記上流の通信装置へ送信するステップと、
をコンピュータに実行させることを特徴とする分散型サービス不能攻撃防止プログラム。

【請求項９】　防御対象であるコンピュータおよびＬＡＮを防御するゲート装置が接続されたネットワークのノードを構成する通信装置上で実行されるコンピュータプログラムであって、
下流のゲート装置又は通信装置から攻撃容疑トラヒックの伝送帯域制限値を受信し、前記攻撃容疑トラヒックの伝送帯域を前記伝送帯域制限値に制限するステップと、
前記受信した伝送帯域制限値と、当該通信装置の１つ上流にある通信装置数とを基に、上流の前記通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限値を算出して、上流の通信装置へ送信するステップと、
前記下流のゲート装置又は通信装置から攻撃容疑トラヒックの平均入力伝送帯域を問い合わせる伝送帯域問合せを受信し、前記攻撃容疑トラヒックの平均入力伝送帯域値を前記下流のゲート装置又は通信装置へ送信するステップと、
前記下流のゲート装置又は通信装置から伝送帯域制限調整値を受信し、前記攻撃容疑トラヒックの伝送帯域を前記伝送帯域制限調整値に制限するステップと、
前記上流の通信装置へ前記攻撃容疑トラヒックの平均入力伝送帯域を問合せを送信するステップと、
前記上流の通信装置から前記攻撃容疑トラヒックの平均入力伝送帯域値を受信するステップと、
前記受信した伝送帯域制限調整値と、前記上流の通信装置から受信した前記攻撃容疑トラヒックの平均入力伝送帯域値とを基に、上流の通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限調整値を算出して前記上流の通信装置へ送信するステップと、
をコンピュータに実行させることを特徴とする分散型サービス不能攻撃防止プログラム。

7

【請求項１０】　前記伝送帯域制限値は、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さをｄ、同一の深さｄにおいてゲート装置または通信装置を識別する番号をｉ、深さｄにあるｉで識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域制限値をＳｓ(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置数をnu(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置を識別するための番号をｋ、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にあるｋで識別される通信装置の攻撃容疑トラヒックの伝送帯域制限値をＳｓ(d+1, i, k)とすると、

【数７】

$$Ss_{(d+1,i,k)} = \frac{1}{nu_{(d,i)}} \quad Ss_{(d,i)}$$

により算出され、

前記伝送帯域制限調整値は、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さをｄ、同一の深さｄにおいてゲート装置または通信装置を識別する番号をｉ、深さｄにあるｉで識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域調整値をＳｓ’(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置数をnu(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置を識別するための番号をｋ、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にあるｋで識別される通信装置から通知された攻撃容疑トラヒックの平均入力伝送帯域値をＢ(d+1, i, k)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にあるｋで識別される通信装置の攻撃容疑トラヒックの伝送帯域制限調整値をＳｓ’(d+1, i, k)とすると、

【数８】

$$Ss'_{(d+1,i,k)} = \frac{B_{(d+1,i,k)}}{nu_{(d,i)} \sum_{l=1} B_{(d+1,i,l)}} \quad Ss'_{(d,i)}$$

により算出されることを特徴とする請求項８または請求項９に記載の分散型サービス不能攻撃防止プログラム。

【請求項１１】　複数の通信装置を網目状に接続してなるネットワークと、防御対象であるコンピュータおよびＬＡＮとの間に介挿されたゲート装置上で実行されるコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体であって、

入力される通信トラヒックをチェックし、分散型サービス不能攻撃の攻撃容疑トラヒックを検出した場合に、当

8

該ゲート装置における前記攻撃容疑トラヒックの伝送帯域制限値と、当該ゲート装置の１つ上流にある通信装置数とを基に、上流の前記通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限値を算出して上流の通信装置へ送信するステップと、

前記上流の通信装置へ前記攻撃容疑トラヒックの平均入力伝送帯域を問合せを送信するステップと、

前記上流の通信装置から前記攻撃容疑トラヒックの平均入力伝送帯域値を受信するステップと、

当該ゲート装置における前記攻撃容疑トラヒックの伝送帯域制限調整値と、前記上流の通信装置から受信した前記攻撃容疑トラヒックの平均入力伝送帯域値とを基に、上流の通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限調整値を算出して前記上流の通信装置へ送信するステップと、

の各処理をコンピュータに実行させる分散型サービス不能攻撃防止プログラムを記録することを特徴とする記録媒体。

【請求項１２】　防御対象であるコンピュータおよびＬＡＮを防御するゲート装置が接続されたネットワークのノードを構成する通信装置上で実行されるコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体であって、

下流のゲート装置又は通信装置から攻撃容疑トラヒックの伝送帯域制限値を受信し、前記攻撃容疑トラヒックの伝送帯域を前記伝送帯域制限値に制限するステップと、

前記受信した伝送帯域制限値と、当該通信装置の１つ上流にある通信装置数とを基に、上流の前記通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限値を算出して、上流の通信装置へ送信するステップと、

前記下流のゲート装置又は通信装置から攻撃容疑トラヒックの平均入力伝送帯域を問い合わせる伝送帯域問合せを受信し、前記攻撃容疑トラヒックの平均入力伝送帯域値を前記下流のゲート装置又は通信装置へ送信するステップと、

前記下流のゲート装置又は通信装置から伝送帯域制限調整値を受信し、前記攻撃容疑トラヒックの伝送帯域を前記伝送帯域制限調整値に制限するステップと、

前記上流の通信装置へ前記攻撃容疑トラヒックの平均入力伝送帯域を問合せを送信するステップと、

前記上流の通信装置から前記攻撃容疑トラヒックの平均入力伝送帯域値を受信するステップと、

前記受信した伝送帯域制限調整値と、前記上流の通信装置から受信した前記攻撃容疑トラヒックの平均入力伝送帯域値とを基に、上流の通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限調整値を算出して前記上流の通信装置へ送信するステップと、

の各処理をコンピュータに実行させる分散型サービス不能攻撃防止プログラムを記録することを特徴とする記録媒体。

【請求項１３】　前記伝送帯域制限値は、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さをｄ、同一の深さｄにおいてゲート装置または通信装置を識別する番号をｉ、深さｄにあるｉで識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域制限値をＳｓ(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置数をnu(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置を識別するための番号をｋ、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にあるｋで識別される通信装置の攻撃容疑トラヒックの伝送帯域制限値をＳｓ(d+1, i, k)とすると、

【数９】

$$Ss_{(d+1,i,k)} = \frac{1}{nu_{(d,i)}} \quad Ss_{(d,i)}$$

により算出され、

前記伝送帯域制限調整値は、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さをｄ、同一の深さｄにおいてゲート装置または通信装置を識別する番号をｉ、深さｄにあるｉで識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域調整値をＳｓ’(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置数をnu(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置を識別するための番号をｋ、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にあるｋで識別される通信装置から通知された攻撃容疑トラヒックの平均入力伝送帯域値をＢ(d+1, i, k)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にあるｋで識別される通信装置の攻撃容疑トラヒックの伝送帯域制限調整値をＳｓ’(d+1, i, k)とすると、

【数１０】

$$Ss'_{(d+1,i,k)} = \frac{B_{(d+1,i,k)}}{\sum_{l=1}^{nu_{(d,i)}} B_{(d+1,i,l)}} \quad Ss'_{(d,i)}$$

により算出されることを特徴とする請求項１１または請求項１２に記載の分散型サービス不能攻撃防止プログラムを記録することを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワークに接続された機器をネットワーク経由での攻撃から防御するための、サービス不能攻撃の防止方法およびその装置ならびにそのコンピュータプログラムに関するものである。

【０００２】

【従来の技術】従来、ＴＣＰ／ＩＰ（Transmission control protocol/internet protocol）などのネットワークプロトコルは、オープンとなっており、互いに信用されるグループで使われるように設計されている。このため、コンピュータのオペレーティングシステムでは、大量の通信トラフィック（データ等）を攻撃目標のサーバに送信することによって、ネットワークの伝送帯域やサーバの資源を消費して正当な利用者の利用を妨げようとするサービス不能攻撃（以下、「ＤｏＳ（Denialof Service）攻撃」と記す）を防ぐことは考慮されていない。このようなＤｏＳ攻撃に対する防御の方法は増えてきているが、複数箇所から同時に連携してＤｏＳ攻撃を行う「ＤＤｏＳ（Distributed Denial of Service）攻撃」に対する防御の方法は未だ効果的な方法が開発されていない。

【０００３】このＤＤｏＳ攻撃に対する一防御の方法として、ＵＵＮＥＴ社のＣｅｎｔｅｒＴｒａｃｋがある。これは、インターネットのルータに診断機能を付加し、ＤＤｏＳ攻撃の送信元を追跡する技術である。

【０００４】また、ＤＤｏＳ攻撃を検出したノードより攻撃元に近い上流ノードで攻撃トラヒックを制限するための技術としては、本出願の発明者等が出願済みの分散型サービス不能攻撃の防止方法（特願２００１－２７４０１６）、ＡＴ＆Ｔ社論文（R. Mahajan, S. M. Bellovin, S. Floyd, J. Ioannidis, V. Paxson and S. Shenker: “Controlling high bandwidth aggregates in the network - extended version”(2001)）、ＩＤＩＰ（Intruder Detection and Isolation Protocol）（D. Schnackenberg, K. Djahandari and D. Sterne: “Infrastructure for intrusion detection and response”, Proceedings of the DARPA Information Survivability Conference and Exposition(DISCEX), South Carolina(2000)）などがある。ＡＴ＆Ｔ社論文及びＩＤＩＰは、攻撃検出イベントを攻撃経路の上流ノードへ伝達し、上流ノードで伝送帯域制限を行うための方式やプロトコルである。本出願の発明者等が出願済みの分散型サービス不能攻撃の防止方法は、ルータにインストールされている移動型パケットフィルタリングプログラムが、自らのプログラムの複製を作成し、その複製を上流ルータ移動させ、各上流ルータへ移動してきた移動型パケットフィルタリングプログラムは、それぞれＤＤｏＳ攻撃者のホストからサーバに向けて送られているトラフィック全てを通過させないようする技術である。

【０００５】

【発明が解決しようとする課題】Ｃｅｎｔｅｒ　Ｔｒａｃｋは、攻撃を受けた被害者が攻撃者を特定することを助ける技術ではあるが、実際に攻撃を受けているときにその攻撃を防御することはできない。加えて、複数箇所

に分散された分散型ＤｏＳの攻撃元になっているコンピュータやそのコンピュータが接続されているネットワークの管理者に連絡をしないと、攻撃そのものを止めることはできないため、実質的には攻撃を止めるまでに何時間、あるいは何日もの時間がかかってしまうという問題点がある。

【０００６】また、この出願の同発明者等が出願済みの分散型サービス不能攻撃の防止方法、ＡＴ＆Ｔ論文及びＩＤＩＰにおては、攻撃パケットと特定されたパケットを次ノードへ送出せず、全て破棄してまう。よって、標的となるサーバのダウンやルータ装置の過負荷等によりサービスが停止する一次被害を防止することはできるが、正規利用者からのパケットを攻撃パケットと識別する方法がないため、誤って正規利用者からの正規パケットも攻撃パケットとして破棄してしまう可能性があり、正規利用者の利用性が低下するといった二次被害を引き起こしてしまうという問題がある。

【０００７】本発明は、上記事情を考慮してなされたものであり、その目的は、正規利用者へのサービス性を低下させる被害を軽減しながらＤＤｏＳ攻撃を防御できる、分散型サービス不能攻撃防止方法及び装置ならびにプログラムを提供することにある。

【０００８】

【課題を解決するための手段】この発明は、上記の課題を解決すべくなされたもので、請求項１に記載の発明は、複数の通信装置を網目状に接続してなるネットワークと、防御対象であるコンピュータおよびＬＡＮと、前記ＬＡＮおよびネットワークの間に介挿されたゲート装置とを有するネットワークシステムにおいて、前記ゲート装置は、入力される通信トラヒックから攻撃容疑トラヒックを検出した場合に、当該ゲート装置における前記攻撃容疑トラヒックの伝送帯域制限値と、当該ゲート装置の１つ上流にある通信装置数とを基に、上流の前記通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限値を算出して上流の前記通信装置へ送信する処理を行い、前記通信装置は、前記攻撃容疑トラヒックの伝送帯域を下流のゲート装置または通信装置から受信した前記伝送帯域制限値に制限すると共に、前記受信した伝送帯域制限値と、当該通信装置の１つ上流にある通信装置数とを基に、上流の前記通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限値を算出して上流の通信装置へ送信する処理を行い、前記攻撃容疑パケット送出元の最上流の前記通信装置に達するまで再帰的に、前記攻撃容疑パケットの伝送帯域の制限と、前記攻撃容疑トラヒックの伝送帯域制限値送信との処理を行い、前記ゲート装置は、前記上流の通信装置へ前記攻撃容疑トラヒックの平均入力伝送帯域を問合せを送信する処理を行い、前記上流の通信装置は、前記下流のゲート装置または通信装置から前記攻撃容疑トラヒックの平均入力伝送帯域問合せを受信して、当該通信装置における前記攻撃容疑トラヒックの平均入力伝送帯域値を前記下流のゲート装置または通信装置へ送信する処理を行い、前記ゲート装置は、当該ゲート装置における前記攻撃容疑トラヒックの伝送帯域制限調整値と、前記上流の通信装置から受信した前記攻撃容疑トラヒックの平均入力伝送帯域値とを基に、上流の通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限調整値を算出して前記上流の通信装置へ送信する処理を行い、前記通信装置は、前記攻撃容疑トラヒックの伝送帯域を下流のゲート装置または通信装置から受信した前記伝送帯域制限調整値に制限すると共に、前記上流の通信装置へ前記攻撃容疑トラヒックの平均入力伝送帯域を問合せを送信する処理と、前記下流の通信装置から受信した伝送帯域制限調整値と、前記上流の通信装置から受信した前記攻撃容疑トラヒックの平均入力伝送帯域値とを基に、上流の通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限調整値を算出して前記上流の通信装置へ送信する処理とを行い、前記攻撃容疑パケット送出元の最上流の前記通信装置に達するまで再帰的に、伝送帯域制限調整値に前記攻撃容疑パケットの伝送帯域の制限と共に、前記攻撃容疑トラヒックの伝送帯域制限調整値の送信との処理を行う、ことを特徴とする分散型サービス不能攻撃防止方法である。

【０００９】請求項２に記載の発明は、請求項１に記載の分散型サービス不能攻撃防止方法であって、前記伝送帯域制限値は、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さをｄ、同一の深さｄにおいてゲート装置または通信装置を識別する番号をｉ、深さｄにあるｉで識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域制限値をＳｓ(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置数をnu(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置を識別するための番号をｋ、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にあるｋで識別される通信装置の攻撃容疑トラヒックの伝送帯域制限値をＳｓ(d+1, i, k)とすると、

【数１１】

$$Ss_{(d+1,i,k)} = \frac{1}{nu_{(d,i)}} \quad Ss_{(d,i)}$$

により算出されることを特徴とする。

【００１０】請求項３に記載の発明は、請求項１または請求項２に記載の分散型サービス不能攻撃防止方法であって、前記伝送帯域制限調整値は、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さをｄ、同一の深さｄにおいてゲート装置または通信装置を識別する番号をｉ、深さｄにあるｉで識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域調整値をＳｓ’(d, i)、深さｄにあるｉで識別

されるゲート装置または通信装置の１つ上流にある通信装置数をnu(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置を識別するための番号をｋ、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にあるｋで識別される通信装置から通知された攻撃容疑トラヒックの平均入力伝送帯域値をＢ(d+1, i, k)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にあるｋで識別される通信装置の攻撃容疑トラヒックの伝送帯域制限調整値をＳｓ’(d+1, i, k)とすると、

【数１２】

$$Ss'_{(d+1,i,k)} = \frac{B_{(d+1,i,k)}}{\sum_{l=1}^{nu_{(d,i)}} B_{(d+1,i,l)}} \quad Ss'_{(d,i)}$$

により算出されることを特徴とする。

【００１１】請求項４に記載の発明は、複数の通信装置を網目状に接続してなるネットワークと、防御対象であるコンピュータおよびＬＡＮとの間に介挿されたゲート装置において、入力される通信トラヒックをチェックし、分散型サービス不能攻撃の攻撃容疑トラヒックを検出するトラヒック監視手段と、当該ゲート装置における前記攻撃容疑トラヒックの伝送帯域制限値と、当該ゲート装置の１つ上流にある通信装置数とを基に、上流の前記通信装置へ通知する前記トラヒック監視手段によって検出された攻撃容疑トラヒックの伝送帯域制限値を算出して上流の通信装置へ送信する帯域制限指示手段と、前記上流の通信装置へ前記攻撃容疑トラヒックの平均入力伝送帯域を問い合わせる伝送帯域問合せ手段と、前記上流の通信装置から前記攻撃容疑トラヒックの平均入力伝送帯域値を受信する伝送帯域値受信手段と、当該ゲート装置における前記攻撃容疑トラヒックの伝送帯域制限調整値と、前記上流の通信装置から受信した前記攻撃容疑トラヒックの平均入力伝送帯域値とを基に、上流の通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限調整値を算出して前記上流の通信装置へ送信する帯域制限調整手段と、を備えることを特徴とするゲート装置である。

【００１２】請求項５に記載の発明は、請求項４に記載のゲート装置であって、前記帯域制限指示手段は、前記伝送帯域制限値を、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さをｄ、同一の深さｄにおいてゲート装置または通信装置を識別する番号をｉ、深さｄにあるｉで識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域制限値をＳｓ(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置数をnu(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置を識別するための番号をｋ、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にあるｋで識別される通信装置の攻撃容疑トラヒックの伝送帯域制限値をＳｓ(d+1, i, k)とすると、

【数１３】

$$Ss_{(d+1,i,k)} = \frac{1}{nu_{(d,i)}} \quad Ss_{(d,i)}$$

により算出し、前記帯域制限調整手段は、前記伝送帯域調整値を、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さをｄ、同一の深さｄにおいてゲート装置または通信装置を識別する番号をｉ、深さｄにあるｉで識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域調整値をＳｓ’(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置数をnu(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置を識別するための番号をｋ、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にあるｋで識別される通信装置から通知された攻撃容疑トラヒックの平均入力伝送帯域値をＢ(d+1, i, k)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にあるｋで識別される通信装置の攻撃容疑トラヒックの伝送帯域制限調整値をＳｓ’(d+1, i, k)とすると、

【数１４】

$$Ss'_{(d+1,i,k)} = \frac{B_{(d+1,i,k)}}{\sum_{l=1}^{nu_{(d,i)}} B_{(d+1,i,l)}} \quad Ss'_{(d,i)}$$

により算出することを特徴とする。

【００１３】請求項６に記載の発明は、防御対象であるコンピュータおよびＬＡＮを防御するゲート装置が接続されたネットワークのノードを構成する通信装置において、下流のゲート装置あるいは通信装置から攻撃容疑トラヒックの伝送帯域制限値を受信し、前記攻撃容疑トラヒックの伝送帯域を前記伝送帯域制限値に制限する帯域制御手段と、前記受信した伝送帯域制限値と、当該通信装置の１つ上流にある通信装置数とを基に、上流の前記通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限値を算出して上流の通信装置へ送信する帯域制限指示手段と、前記下流のゲート装置あるいは通信装置から前記攻撃容疑トラヒックの平均入力伝送帯域問い合わせを受信し、当該通信装置における前記攻撃容疑トラヒックの平均入力伝送帯域値を前記下流のゲート装置あるいは通信装置へ送信する帯域通知手段と、前記下流のゲート装置あるいは通信装置から攻撃容疑トラヒックの伝送帯域制限調整値を受信し、前記攻撃容疑トラヒックの伝

15

送帯域を前記伝送帯域制限調整値に制限する帯域制御調整手段と、前記上流の通信装置へ前記攻撃容疑トラヒックの平均入力伝送帯域を問い合わせる伝送帯域問合せ手段と、前記上流の通信装置から前記攻撃容疑トラヒックの平均入力伝送帯域値を受信する伝送帯域値受信手段と、前記上流の通信装置から受信した前記攻撃容疑トラヒックの平均入力伝送帯域値と前記受信した伝送帯域制限調整値とを基に、上流の通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限調整値を算出して、前記上流の通信装置へ送信する帯域制限調整手段と、を備えることを特徴とする通信装置である。

【００１４】請求項７に記載の発明は、請求項６に記載の通信装置であって、前記帯域制限指示手段は、前記伝送帯域制限値を、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さをｄ、同一の深さｄにおいてゲート装置または通信装置を識別する番号をｉ、深さｄにあるｉで識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域制限値をＳｓ(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置数をnu(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置を識別するための番号をｋ、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にあるｋで識別される通信装置の攻撃容疑トラヒックの伝送帯域制限値をＳｓ(d+1, i, k)とすると、

【数１５】

$$Ss_{(d+1,i,k)} = \frac{1}{nu_{(d,i)}} \quad Ss_{(d,i)}$$

により算出し、前記帯域制限調整手段は、前記伝送帯域調整値を、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さをｄ、同一の深さｄにおいてゲート装置または通信装置を識別する番号をｉ、深さｄにあるｉで識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域調整値をＳｓ’(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置数をnu(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置を識別するための番号をｋ、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にあるｋで識別される通信装置から通知された攻撃容疑トラヒックの平均入力伝送帯域値をＢ(d+1, i, k)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にあるｋで識別される通信装置の攻撃容疑トラヒックの伝送帯域制限調整値をＳｓ’(d+1, i, k)とすると、

【数１６】

16

$$Ss'_{(d+1,i,k)} = \frac{B_{(d+1,i,k)}}{\sum_{l=1}^{nu_{(d,i)}} B_{(d+1,i,l)}} \quad Ss'_{(d,i)}$$

により算出することを特徴とする。

【００１５】請求項８に記載の発明は、複数の通信装置を網目状に接続してなるネットワークと、防御対象であるコンピュータおよびＬＡＮとの間に介挿されたゲート装置上で実行されるコンピュータプログラムであって、入力される通信トラヒックをチェックし、分散型サービス不能攻撃の攻撃容疑トラヒックを検出した場合に、当該ゲート装置における前記攻撃容疑トラヒックの伝送帯域制限値と、当該ゲート装置の１つ上流にある通信装置数とを基に、上流の前記通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限値を算出して上流の通信装置へ送信するステップと、前記上流の通信装置へ前記攻撃容疑トラヒックの平均入力伝送帯域を問合せを送信するステップと、前記上流の通信装置から前記攻撃容疑トラヒックの平均入力伝送帯域値を受信するステップと、当該ゲート装置における前記攻撃容疑トラヒックの伝送帯域制限調整値と、前記上流の通信装置から受信した前記攻撃容疑トラヒックの平均入力伝送帯域値とを基に、上流の通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限調整値を算出して前記上流の通信装置へ送信するステップと、をコンピュータに実行させることを特徴とする分散型サービス不能攻撃防止プログラムである。

【００１６】請求項９に記載の発明は、防御対象であるコンピュータおよびＬＡＮを防御するゲート装置が接続されるたネットワークのノードを構成する通信装置上で実行されるコンピュータプログラムであって、下流のゲート装置又は通信装置から攻撃容疑トラヒックの伝送帯域制限値を受信し、前記攻撃容疑トラヒックの伝送帯域を前記伝送帯域制限値に制限するステップと、前記受信した伝送帯域制限値と、当該通信装置の１つ上流にある通信装置数とを基に、上流の前記通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限値を算出して、上流の通信装置へ送信するステップと、前記下流のゲート装置又は通信装置から攻撃容疑トラヒックの平均入力伝送帯域を問い合わせる伝送帯域問合せを受信し、前記攻撃容疑トラヒックの平均入力伝送帯域値を前記下流のゲート装置又は通信装置へ送信するステップと、前記下流のゲート装置又は通信装置から伝送帯域制限調整値を受信し、前記攻撃容疑トラヒックの伝送帯域を前記伝送帯域制限調整値に制限するステップと、前記上流の通信装置へ前記攻撃容疑トラヒックの平均入力伝送帯域を問合せを送信するステップと、前記上流の通信装置から前記攻撃容疑トラヒックの平均入力伝送帯域値を受信するステップと、前記受信した伝送帯域制限調整値と、前記上

流の通信装置から受信した前記攻撃容疑トラヒックの平均入力伝送帯域値とを基に、上流の通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限調整値を算出して前記上流の通信装置へ送信するステップと、をコンピュータに実行させることを特徴とする分散型サービス不能攻撃防止プログラムである。

【００１７】請求項１０に記載の発明は、請求項８または請求項９に記載の分散型サービス不能攻撃防止プログラムであって、前記伝送帯域制限値は、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さをｄ、同一の深さｄにおいてゲート装置または通信装置を識別する番号をｉ、深さｄにあるｉで識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域制限値をＳｓ(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置数をnu(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置を識別するための番号をｋ、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にあるｋで識別される通信装置の攻撃容疑トラヒックの伝送帯域制限値をＳｓ(d+1, i, k)とすると、

【数１７】

$$Ss_{(d+1,i,k)} = \frac{1}{nu_{(d,i)}} \quad Ss_{(d,i)}$$

により算出され、前記伝送帯域制限調整値は、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さをｄ、同一の深さｄにおいてゲート装置または通信装置を識別する番号をｉ、深さｄにあるｉで識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域調整値をＳｓ’(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置数をnu(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置を識別するための番号をｋ、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にあるｋで識別される通信装置から通知された攻撃容疑トラヒックの平均入力伝送帯域値をＢ(d+1, i, k)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にあるｋで識別される通信装置の攻撃容疑トラヒックの伝送帯域制限調整値をＳｓ’(d+1, i, k)とすると、

【数１８】

$$Ss'_{(d+1,i,k)} = \frac{B_{(d+1,i,k)}}{nu_{(d,i)} \sum_{l=1} B_{(d+1,i,l)}} \quad Ss'_{(d,i)}$$

により算出されることを特徴とする。

【００１８】請求項１１に記載の発明は、複数の通信装置を網目状に接続してなるネットワークと、防御対象であるコンピュータおよびＬＡＮとの間に介挿されたゲート装置上で実行されるコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体であって、入力される通信トラヒックをチェックし、分散型サービス不能攻撃の攻撃容疑トラヒックを検出した場合に、当該ゲート装置における前記攻撃容疑トラヒックの伝送帯域制限値と、当該ゲート装置の１つ上流にある通信装置数とを基に、上流の前記通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限値を算出して上流の通信装置へ送信するステップと、前記上流の通信装置へ前記攻撃容疑トラヒックの平均入力伝送帯域を問合せを送信するステップと、前記上流の通信装置から前記攻撃容疑トラヒックの平均入力伝送帯域値を受信するステップと、当該ゲート装置における前記攻撃容疑トラヒックの伝送帯域制限調整値と、前記上流の通信装置から受信した前記攻撃容疑トラヒックの平均入力伝送帯域値とを基に、上流の通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限調整値を算出して前記上流の通信装置へ送信するステップと、の各処理をコンピュータに実行させる分散型サービス不能攻撃防止プログラムを記録することを特徴とする記録媒体である。

【００１９】請求項１２に記載の発明は、防御対象であるコンピュータおよびＬＡＮを防御するゲート装置が接続されたネットワークのノードを構成する通信装置上で実行されるコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体であって、下流のゲート装置又は通信装置から攻撃容疑トラヒックの伝送帯域制限値を受信し、前記攻撃容疑トラヒックの伝送帯域を前記伝送帯域制限値に制限するステップと、前記受信した伝送帯域制限値と、当該通信装置の１つ上流にある通信装置数とを基に、上流の前記通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限値を算出して、上流の通信装置へ送信するステップと、前記下流のゲート装置又は通信装置から攻撃容疑トラヒックの平均入力伝送帯域を問い合わせる伝送帯域問合せを受信し、前記攻撃容疑トラヒックの平均入力伝送帯域値を前記下流のゲート装置又は通信装置へ送信するステップと、前記下流のゲート装置又は通信装置から伝送帯域制限調整値を受信し、前記攻撃容疑トラヒックの伝送帯域を前記伝送帯域制限調整値に制限するステップと、前記上流の通信装置へ前記攻撃容疑トラヒックの平均入力伝送帯域を問合せを送信するステップと、前記上流の通信装置から前記攻撃容疑トラヒックの平均入力伝送帯域値を受信するステップと、前記受信した伝送帯域制限調整値と、前記上流の通信装置から受信した前記攻撃容疑トラヒックの平均入力伝送帯域値とを基に、上流の通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限調整値を算出して前記上流の通信装置へ送信するステップと、の各処理をコンピュータに実行させる分散型サービス不能攻撃防止プロ

グラムを記録することを特徴とする記録媒体である。

【００２０】請求項１３に記載の発明は、請求項１１または請求項１２に記載の分散型サービス不能攻撃防止プログラムを記録することを特徴とする記録媒体であって、前記伝送帯域制限値は、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さをｄ、同一の深さｄにおいてゲート装置または通信装置を識別する番号をｉ、深さｄにあるｉで識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域制限値をＳｓ(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置数をnu(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置を識別するための番号をｋ、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にあるｋで識別される通信装置の攻撃容疑トラヒックの伝送帯域制限値をＳｓ(d+1, i, k)とすると、

【数１９】

$$Ss_{(d+1,i,k)} = \frac{1}{nu_{(d,i)}} \quad Ss_{(d,i)}$$

により算出され、前記伝送帯域制限調整値は、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さをｄ、同一の深さｄにおいてゲート装置または通信装置を識別する番号をｉ、深さｄにあるｉで識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域調整値をＳｓ’(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置数をnu(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置を識別するための番号をｋ、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にあるｋで識別される通信装置から通知された攻撃容疑トラヒックの平均入力伝送帯域値をＢ(d+1, i, k)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にあるｋで識別される通信装置の攻撃容疑トラヒックの伝送帯域制限調整値をＳｓ’(d+1, i, k)とすると、

【数２０】

$$Ss'_{(d+1,i,k)} = \frac{B_{(d+1,i,k)}}{nu_{(d,i)} \sum_{l=1} B_{(d+1,i,l)}} \quad Ss'_{(d,i)}$$

により算出されることを特徴とする。

【００２１】

【発明の実施の形態】以下図面を参照し、この発明の一実施の形態について説明する。図１は、同実施の形態を適用したネットワークの構成図である。この図において、２０００はサーバ、２００１はこの発明の一実施形

態によるゲート装置（ゲートウェイ）、２００２～２００６はこの発明の一実施形態による通信装置（ルータ）、２００７～２０１０は端末装置である。ＤＤｏＳ攻撃の被攻撃者のサーバ２０００が収容されているＬＡＮ（ローカルエリアネットワーク）は、ゲート装置２００１によって外部のネットワークに接続されている。そして、ネットワークは通信装置２００２、２００３、２００４、２００５、２００６を有している。ＤＤｏＳ攻撃者によって操作された端末装置２００７、２００８が、攻撃パケットを被攻撃者のサーバ２０００に向かって送信すると、攻撃パケットが被攻撃者収容ＬＡＮに集中して混雑が発生することにより、ゲート装置２００１の資源を消費してしまい、ＤＤｏＳ攻撃者とは無関係な正規利用者の端末２００９、２０１０からサーバ２０００に接続できなくなるという現象が起こる。

【００２２】ゲート装置２００１は、予めサーバ２０００を保有する利用者が設定した攻撃容疑検出条件を記憶している。図２に攻撃容疑検出条件の設定の例を示す。さらに、ゲート装置２００１は、防御対象のサーバ２０００及びサーバ２０００が収容されているＬＡＮの所有者によって予め設定された伝送帯域制限値を記憶している。

【００２３】図２における攻撃容疑検出条件は、検出属性、検出閾値及び検出間隔の組からなる３組のレコードで構成される。ここでは、番号はレコードを特定するために便宜上使用される。攻撃容疑検出条件は、受信パケットが攻撃パケットである可能性がある攻撃容疑パケットを検出するために使用され、３組のレコードの内のいずれかのレコードの条件にトラヒックが一致した場合、このトラヒックの通信パケットは攻撃容疑パケットであると認識される。検出属性は、ＩＰパケットの第３／４層属性種別とそれら属性値の組を指定するが、第３層属性であるＩＰの「Destination IP Address（宛先ＩＰアドレス）」という属性種別は必ず指定される。図２において、番号１のレコードの検出属性は、「Destination IP Address（宛先ＩＰアドレス）」が「192.168.1.1/32」であり（dst=192.168.1.1/32）、ＩＰの上位層（第４層）のプロトコル種別を示す「Protocol（プロトコル）」が「ＴＣＰ」であり（Protocol=TCP）、かつ、第４層プロトコルがどのアプリケーションの情報かを示す「Destination Port（宛先ポート番号）」が「８０」である（Port=80）という属性種別とそれら属性値の組で指定される。番号２のレコード検出属性は、「Destination IP Address（宛先ＩＰアドレス）」が「192.168.1.2/32」であり（dst=192.168.1.2/32）、かつ、「Protocol（プロトコル）」が「ＵＤＰ（User Datagram protocol）」である（Protocol=UDP）という属性種別とそれら属性値の組で指定される。また、番号３のレコード検出属性は、「Destination IP Address（宛先ＩＰアドレス）」が「192.168.1.0/24」である属性種別とその属性

値で指定される。検出閾値は、同じレコードで指定される検出属性を持つ受信パケットのトラヒックを攻撃容疑トラヒックとして検出するための最低の伝送帯域を、検出間隔は同じく最低の連続時間を示している。

【００２４】また、ゲート装置２００１及び通信装置２００２～２００６は、攻撃容疑パケットのトラヒックを分析し、不正トラヒックを検出するための不正トラヒック検出条件を保有する。図３に不正トラヒック検出条件の設定の例を示す。ここでは、番号はレコードを特定するために便宜上使用される。不正トラヒック条件は、既知のＤＤｏＳ攻撃の複数のトラヒックパターンから構成され、攻撃容疑パケットのトラヒックがいずれかのトラヒックパターンに合致した場合に、不正トラヒックであると認識される。図３の番号１の不正トラヒック条件は、「伝送帯域Ｔ１Ｋｂｐｓ以上のパケットがＳ１秒以上連続送信されている」というトラヒックパターンを示している。また、番号２の不正トラヒック条件は、「伝送帯域Ｔ２Ｋｂｐｓ以上、第３層プロトコルであるＩＣＭＰ（Internet Control Message Protocol）上のエコー応答（Echo Reply）メッセージのパケットがＳ２秒以上連続送信されている」というトラヒックパターンを示している。番号３の不正トラヒック条件は、「伝送帯域Ｔ３Ｋｂｐｓ以上、データが長すぎるためパケットに含まれるデータは複数ＩＰパケットに分割して送信していることを示すフラグメントパケットがＳ３秒以上連続送信されている」というトラヒックパターンを示している。

【００２５】ここで、ゲート装置２００１及び通信装置２００２～２００６が備える帯域制御モデルを説明する。図４は本実施の形態におけるゲート装置２００１及び通信装置２００２～２００６が備える帯域制御モデルを示す。帯域制御モデルは、入力パケットをクラス別に分類し、このクラスに従ってパケットの出力帯域制御を実現するためのモデルを示す。フィルタ２０２１は、入力されたパケットを正規クラス２０２２、容疑クラス２０２６、不正クラス２０２４の３つのクラスに分類する。なお、このフィルタ２０２１の分類アルゴリズムは後述する。正規クラス２０２２はデフォルトクラスであり、正規クラス２０２２に分類されたパケットは正規キュー２０２３につながれ、伝送帯域を制限せずに出力される。容疑クラス２０２６に分類されたパケットは、容疑パケットか否かを判断するための防御対象のサーバ２０００及びサーバ２０００が収容されているＬＡＮ毎に発生する容疑キュー２０２７につながれ、防御対象のサーバ２０００及びサーバ２０００が収容されているＬＡＮの所有者によって予め設定された伝送帯域制限値に出力伝送帯域が制限される。なお、容疑シグネチャの生成については後述する。サーバ２０００を収容しているゲート装置２００１の容疑キューの伝送帯域制限値は防御対象のサーバ２０００及びサーバ２０００が収容されているＬＡＮの所有者によって予め設定された伝送帯域制限値を使用するが、上流の通信装置２００２～２００６では、下流の通信装置から受信した伝送帯域制限値を使用する。不正クラス２０２４に分類されたパケットは、不正キュー２０２５につながれ、サーバ所有者やネットワークのポリシーに関わらず、０または０に近い伝送帯域に制限される。

【００２６】続いて、ゲート装置２００１及び通信装置２００２～２００６が伝送帯域制限を実行するための、フィルタ２０２１の分類アルゴリズムについて説明する。ゲート装置２００１及び通信装置２００２～２００６は、当該通信装置に入力される全ての通信パケットをこの分類アルゴリズムで分類する。図５はフィルタ２０２１における分類アルゴリズムを示す。まず、ステップＳ３００３において、フィルタ２０２１は、入力されたパケットが不正シグネチャと合致するか判断する。不正シグネチャに合致した場合、パケットは不正クラス２０２４に分類される（ステップＳ３００４）。不正シグネチャに合致しなかった場合は、ステップＳ３００５に進み、パケットが容疑シグネチャであるか判断し、容疑シグネチャに合致すれば容疑クラス２０２６へ分類され（ステップＳ３００６）、合致しない場合には正規クラス２０２２へ分類される（ステップＳ３００７）。このようにして各クラスに分類されたパケットは、正規キューであれば伝送帯域を制限せずに出力され、容疑キュー及び不正キューであればそれぞれの伝送帯域制限値に従って伝送帯域が制限されて出力される。なお、容疑シグネチャ及び不正シグネチャの生成については後述する。

【００２７】次に、ＤＤｏＳ攻撃に対する対策方式の処理手順を示す。まず、図６のゲート装置２００１の攻撃容疑パケット検出時の動作を示すフローチャート、図８の通信装置２００２、２００３の伝送帯域制限指示受信時の動作を示すフローチャート及び図９のゲート装置２００１及び通信装置２００２～２００６の不正トラヒック検出時の動作を示すフローチャートを用いてＤＤｏＳ攻撃発生と同時に初期の伝送帯域制限を実施する処理手順を説明する。

【００２８】図６のステップＳ３０１１において、ゲート装置２００１は、攻撃容疑検出条件（図２）に従って、検出間隔で指定されているより長い時間連続して、検出閾値で指定されている以上の伝送帯域を使用している、検出属性に合致するトラヒックをチェックし、３組のレコードの内のいずれかのレコードに合致した場合、このトラヒックを攻撃容疑トラヒックとして検出する。すると、ステップＳ３０１２において、この検出された攻撃容疑トラヒックが満たしている攻撃容疑検出条件のレコードの検出属性を、容疑シグネチャとして生成する。容疑シグネチャは、攻撃容疑トラヒックの通信パケット、すなわち攻撃容疑パケットを識別するために用いられる。例えば、図２の設定例を用いて説明すると、番

号１のレコードの条件で検出されるパケットの容疑シグネチャは{dst=192.168.1.1/32, Protocol=TCP, Port=80}となる。

【００２９】次いで、ステップＳ３０１３において、ゲート装置２００１は、ステップＳ３０１２において生成した容疑シグネチャをフィルタ２０２１に登録する。次に、防御対象のサーバ２０００及びサーバ２０００が収容されているＬＡＮの所有者によって予め設定された伝送帯域制限値に攻撃容疑トラヒックの伝送帯域を制限するための容疑キュー２０２７を生成する。なお、同一防御対象に関する容疑キューが既に生成済みの場合は、新たな容疑キューの生成は行わない。これにより、以後、図４に示す帯域制御モデルと図５に示すフィルタ２０２１の分類アルゴリズムに従って、容疑シグネチャに合致する攻撃容疑パケットの伝送帯域の制限が実行される。

【００３０】そして、ゲート装置２００１は、ステップＳ３０１４において、容疑シグネチャと算出した攻撃容疑パケットの伝送帯域制限値とを含んだ伝送帯域制限指示を１つ上流にある通信装置２００２、２００３に送信する。ここで、伝送帯域制限値の算出方法を説明する。なお、本明細書においては、ゲート装置あるいは通信装置を識別するための添え字を持つ

【数２１】

$$Ss_{(d+1,i,k)}\ ,\quad Ss_{(d,i)}\ ,\quad nu_{(d,i)}$$

などの変数を便宜上Ｓｓ(d+1, i, k)、Ｓｓ(d, i)、nu(d, i)のように記述する。ネットワークにおいて、ゲート装置２００１の存在する階層を初期値０として通信装置がゲート装置２００１から何ホップ目に存在するかを示す階層の深さをｄ、同一の深さｄにおいてゲート装置または通信装置を識別する番号をｉ、深さｄにあるｉで識別される通信装置の攻撃容疑パケットの伝送帯域制限値をＳｓ(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流（すなわち深さｄ＋１）にある通信装置数をnu(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流（深さｄ＋１）にある通信装置を識別するための番号をｋ、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流（深さｄ＋１）にあるｋで識別される通信装置の攻撃容疑トラヒックの伝送帯域制限値をＳｓ(d+1, i, k)とする。このとき、伝送帯域制限値は、以下の式で算出される。

【数２２】

$$Ss_{(d+1,i,k)} = \frac{1}{nu_{(d,i)}}\ Ss_{(d,i)}$$

よって、ゲート装置２００１は、上記の式により、通信装置２００２、２００３に指示する伝送帯域制限値を算出する。これは、ゲート装置２００１は、自身が持つ伝送帯域制限値を１つ上流の通信装置全てに均等に割り当

てることを示す。図７は図１の構成における伝送帯域制限値の算出の例を示す図である。この図において、ゲート装置２００１は深さｄ＝０であり、この深さｄ＝０には１つの装置のみが存在するためゲート装置２００１のｉは１である。ゲート装置２００１の伝送帯域制限値の初期値Ｓｓ(0, 1)は、攻撃容疑トラヒックを検出したときのレコードに対応した伝送帯域制限値である。ここでは例として、伝送帯域制限値が８００ｋｂｐｓであったとする。そして、ゲート装置２００１には２つの１つ上流の通信装置２００２、２００３が存在するため、１つ上流の通信装置数nu(0, 1)は２である。よって、ゲート装置２００１には、１番目の１つ上流の通信装置２００２の伝送帯域制限値Ｓｓ(1, 1, 1)及び２番目の１つ上流の通信装置２００３の伝送帯域制限値Ｓｓ(1, 1, 2)は、Ｓｓ(0, 1)＝８００ｋｂｐｓをnu(0, 1)＝２で除算した４００ｋｂｐｓとなる。

【００３１】次に、伝送帯域制限指示受信時の通信装置２００２、２００３の動作を説明する。図８のステップＳ３０２１において、通信装置２００２、２００３は、ゲート装置２００１が送信した（ステップＳ３０１４）伝送帯域制限指示を受信する。次に、ステップＳ３０２２に進み、通信装置２００２、２００３は、受信した伝送帯域制限指示に含まれる容疑シグネチャをフィルタ２０２１に登録し、容疑シグネチャ及び攻撃容疑パケットの伝送帯域制限値に対応した容疑キュー２０２７を生成する。これにより、以後、図４に示す帯域制御モデルと図５に示すフィルタ２０２１の分類アルゴリズムに従って容疑シグネチャに合致する攻撃容疑パケットの伝送帯域の制限が実行される。

【００３２】通信装置２００２はステップＳ３０２３において、その上流にある通信装置２００４に、通信装置２００３はその上流にある通信装置２００５及び２００６に、受信した容疑シグネチャと、受信した伝送帯域制限値から算出した伝送帯域制限値とを含んだ伝送帯域制限指示を送信する。このときの算出方法は、ゲート装置２００１のステップＳ３００３と同様である。すなわち、通信装置２００２、２００３は、ゲート装置２００１から受信した伝送帯域制限値を１つ上流の通信装置全てに均等に割り当てる。図７を用いて説明すると、通信装置２００２、２００３の深さｄは１であり、この深さｄ＝１には２つの通信装置が存在し、その１番目の通信装置２００２のｉは１、２番目の通信装置２００３のｉは２である。通信装置２００２の伝送帯域制限値Ｓｓ(1, 1)及び通信装置２００３の伝送帯域制限値Ｓｓ(1, 2)は、それぞれゲート装置２００１から受信した伝送帯域制限値Ｓｓ(1, 1, 1)、Ｓｓ(1, 1, 2)であり、すなわち４００ｋｂｐｓである。そして、通信装置２００２には１つの上流の通信装置２００４が存在するため、１つ上流の通信装置数nu(1, 1)は１である。よって、通信装置２００４の伝送帯域制限値Ｓｓ(2, 1, 1)は、Ｓｓ(1, 1)＝４０

０ｋｂｐｓをnu(1,1)＝１で除算した４００ｋｂｐｓとなる。一方、通信装置２００３には２つの上流の通信装置２００５、２００６が存在するため１つ上流の通信装置数nu(1,2)は２である。よって、通信装置２００５の伝送帯域制限値Ｓｓ(2,2,1)及び通信装置２００６の伝送帯域制限値Ｓｓ(2,2,2)は、Ｓｓ(1,2)＝４００ｋｂｐｓをnu(1,2)＝２で除算した２００ｋｂｐｓとなる。

【００３３】そして、通信装置２００４は通信装置２００２から、通信装置２００５、２００６は通信装置２００３から伝送帯域制限指示を受信し、通信装置２００２、２００３におけるステップＳ３０２１～Ｓ３０２２と同様に動作する。通信装置２００４～２００６は、ルーチングテーブルなどにより上流に通信装置がないと判断できるため、ステップＳ３０２３は実行しない。

【００３４】次に、ゲート装置２００１及び通信装置２００２～２００６の不正トラヒック検出時の動作を説明する。図９のステップＳ３０３１において、ゲート装置２００１及び通信装置２００２～２００６は、ＤＤｏＳ攻撃者がパケットを送出しているネットワークを特定するため入力パケットを分析して、不正トラヒック条件のいずれかのパターンに合致するトラヒックを検出する。すると、ゲート装置２００１及び通信装置２００２～２００６は、ステップＳ３０３２において、この検出された不正トラヒック条件を満たすパケットの送信元ＩＰアドレスを不正アドレス範囲として特定し、この不正アドレス範囲であり、かつ、容疑シグネチャに合致するという条件を不正シグネチャとする。そして、ゲート装置２００１及び通信装置２００２～２００６は、ステップＳ３０３３においてこの不正シグネチャをフィルタ２０２１に登録する。これにより、以後、図４に示す帯域制御モデルと図５に示すフィルタ２０２１の分類アルゴリズムに従って不正シグネチャで識別される攻撃パケットの伝送帯域はさらに制限される。すなわち、攻撃パケットは不正クラス２０２４に分類され、正規利用者からのパケットである正規パケットのみが攻撃容疑パケットとして容疑クラス２０２６に分類される。

【００３５】以上説明した初期の伝送帯域制限を実施することにより、早期にネットワークの伝送帯域の溢れを防いだ後、攻撃容疑パケットの入力トラヒックに応じて、伝送帯域制限値の調整を実施する処理手順を説明する。図１０は伝送帯域制限調整値の算出の例、図１１はゲート装置２００１及び通信装置２００２～２００６の伝送帯域制限値の調整の動作を示すフローチャートである。

【００３６】図１０において、図７に示す初期の伝送帯域制限後、端末装置２００７から２Ｍｂｐｓ、端末装置２００８から２Ｍｂｐｓの攻撃パケットが送信されており、また、端末装置２００９から６００ｋｂｐｓ、端末装置２０１０からは１００ｋｂｐｓの攻撃容疑パケットが送信されている。

【００３７】通信装置２００４は、端末装置２００７から入力される攻撃パケットを不正クラス２０２４に分類しており、当該通信装置２００４に入力される全攻撃容疑トラヒックは端末装置２００９から受信される６００ｋｂｐｓである。これは、初期の伝送帯域制限の手順で受信した伝送帯域制限値Ｓｓ(2,1,1)＝４００ｋｂｐｓより大きいため、下流の通信装置２００２には、攻撃容疑トラヒックを４００ｋｂｐｓに帯域制限して出力している。通信装置２００２は、上流の通信装置２００４から入力される攻撃容疑トラヒックの伝送帯域が４００ｋｂｐｓであり、初期の伝送帯域制限の手順で受信した伝送帯域制限値Ｓｓ(1,1,1)＝４００ｋｂｐｓ以下であるため、下流のゲート装置２００１には４００ｋｂｐｓの攻撃容疑トラヒックを出力している。

【００３８】一方、通信装置２００５は、端末装置２００８から入力される攻撃パケットを不正クラス２０２４に分類しているため、下流の通信装置２００３に出力している攻撃容疑トラヒックは０ｋｂｐｓである。また、通信装置２００６に入力される攻撃容疑トラヒックは、端末装置２０１０から受信される１００ｋｂｐｓである。これは初期の伝送帯域制限の手順で受信した伝送帯域制限値Ｓｓ(2,2,2)＝２００ｋｂｐｓ以下であるため、下流の通信装置２００３には、そのまま１００ｋｂｐｓの攻撃容疑トラヒックを出力している。よって、通信装置２００３は、上流の通信装置２００５、２００６から入力される攻撃容疑トラヒックの伝送帯域の合計が１００ｋｂｐｓと、初期の伝送帯域制限の手順で受信した伝送帯域制限値Ｓｓ(1,1,2)＝４００ｋｂｐｓ以下であるため、下流のゲート装置２００１には１００ｋｂｐｓの攻撃容疑トラヒックを出力している。

【００３９】図１１のステップＳ３０４１において、ゲート装置２００１は、初期伝送帯域制限実施から一定時間後、全上流の通信装置２００２、２００３に当該ゲート装置２００１に入力される攻撃容疑トラヒックの平均入力伝送帯域を問い合わせる。すると、ステップＳ３０５１において、通信装置２００２、２００３は、平均入力伝送帯域の問合せを受信する。そして、ステップＳ３０５２において、通信装置２００２、２００３は、自身の攻撃容疑トラヒックの平均入力伝送帯域値をゲート装置２００１に通知する。

【００４０】次に、ステップＳ３０４２においてゲート装置２００１は、通信装置２００２，２００３から攻撃容疑トラヒックの平均入力伝送帯域値を受信する。すると、ステップＳ３０４３において、ゲート装置２００１は、受信した平均入力伝送帯域値を基に算出した攻撃容疑パケットの伝送帯域制限調整値を含んだ伝送帯域制限調整指示を、全上流の通信装置２００２、２００３に送信する。ここで、伝送帯域制限値の算出方法を説明する。なお、本明細書においては、ゲート装置あるいは通信装置を識別するための添え字を持つ

【数２３】

$$Ss'_{(d+1,i,k)} \quad , B_{(d+1,i,k)} \quad , T_{(d,i)} \quad , \quad Ss'_{(d,i)}$$

などの変数を便宜上Ｓｓ’(d+1, i, k)、Ｂ(d+1, i, k)、Ｓｓ’(d, i)のように記述する。ネットワークにおいて、ゲート装置２００１の存在する階層を初期値０として通信装置がゲート装置２００１から何ホップ目に存在するかを示す階層の深さをｄ、同一の深さｄにおいてゲート装置または通信装置を識別する番号をｉ、深さｄにあるｉで識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域調整値をＳｓ’(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にある通信装置数をnu(d, i)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にあるｋで識別される通信装置の攻撃容疑トラヒックの平均入力伝送帯域値Ｂ(d+1, i, k)、深さｄにあるｉで識別されるゲート装置または通信装置の１つ上流にあるｋで識別される通信装置の攻撃容疑トラヒックの伝送帯域制限調整値Ｓｓ’(d+1, i, k)とする。このとき、伝送帯域制限調整値は、以下の式で算出される。

【数２４】

$$Ss'_{(d+1,i,k)} = \frac{B_{(d+1,i,k)}}{\sum_{l=1}^{nu_{(d,i)}} B_{(d+1,i,l)}} Ss'_{(d,i)}$$

よって、ゲート装置２００１は、上記の式により、通信装置２００２、２００３に指示する伝送帯域制限調整値を算出する。これは、ゲート装置２００１は、上流の通信装置の攻撃容疑トラヒックの平均入力伝送帯域の比率に従って、攻撃容疑トラヒックの伝送帯域値を調整することを示している。ただし、ゲート装置２００１の伝送帯域制限調整値の初期値Ｓｓ’(0, 1)は伝送帯域制限値の初期値Ｓｓ(0, 1)と同じである。

【００４１】図１０の送帯域制限調整値の算出の例を用いて説明する。ゲート装置２００１の１番目の１つ上流の通信装置２００２からゲート装置２００１に入力される攻撃容疑トラヒックの平均入力伝送帯域値Ｂ(1, 1, 1)は４００ｋｂｐｓ、２番目の１つ上流の通信装置２００３からゲート装置２００１に入力される攻撃容疑トラヒックの平均入力伝送帯域値Ｂ(1, 1, 2)は１００ｋｂｐｓである。よって、（数２４）の右辺の分母は、全上流の通信装置からの平均入力伝送帯域値の合計を示していることより、Ｂ(1, 1, 1)＋Ｂ(1, 1, 2)＝５００ｋｂｐｓと算出される。また、伝送帯域制限調整値の初期値Ｓｓ’(0, 1)＝Ｓｓ(0, 1)であるため、図７の例より、Ｓｓ’(0, 1)は８００ｋｂｐｓである。従って、１番目の１つ上流の通信装置２００２の攻撃容疑トラヒックの伝送帯域制限調整値Ｓｓ’(1, 1, 1)は、Ｂ(1, 1, 1)＝４００ｋｂｐｓを分母５００ｋｂｐｓで除算し、伝送帯域制限調整値の初期値Ｓｓ’(0, 1)＝８００ｋｂｐｓを乗算した６４０ｋｂｐｓとなる。一方、２番目の１つ上流の通信装置２００３の攻撃容疑トラヒックの伝送帯域制限調整値Ｓｓ’(1, 1, 2)は、Ｂ(1, 1, 2)＝１００ｋｂｐｓを分母５００ｋｂｐｓで除算し、伝送帯域制限調整値の初期値Ｓｓ’(0, 1)＝８００ｋｂｐｓを乗算した１６０ｋｂｐｓとなる。

【００４２】そして、図１１のステップＳ３０５３において、通信装置２００２、２００３は、ゲート装置２００１から伝送帯域制限調整指示を受信する。すると、ステップＳ３０５４に進み、通信装置２００２、２００３は、容疑キュー２０２７の伝送帯域制限値を受信した伝送帯域制限調整指示に含まれる伝送帯域制限調整値に変更する。これにより、以後、図４に示す帯域制御モデルと図５に示すフィルタ２０２１の分類アルゴリズムに従って容疑シグネチャに合致する攻撃容疑パケットの伝送帯域は伝送帯域制限調整値に制限される。

【００４３】次に、図１１のステップ３０５５へ進み、通信装置２００２はその上流にある通信装置２００４に当該通信装置２００２に入力される攻撃容疑トラヒックの平均入力伝送帯域を、通信装置２００３はその上流にある通信装置２００５及び２００６に当該通信装置２００３に入力される攻撃容疑トラヒックの平均入力伝送帯域を問い合わせる。通信装置２００４～２００６は、ステップＳ３０６１において、平均入力伝送帯域の問合せを受信する。するとステップＳ３０６２において、通信装置２００４は、通信装置２００２に、通信装置２００５、２００６は、通信装置２００３に自身の攻撃容疑トラヒックの平均入力伝送帯域値を通知する。

【００４４】続いて、ステップＳ３０５６において、通信装置２００２、２００３は、通信装置２００４～２００６から受信した平均入力伝送帯域値を受信する。すると、ステップＳ３０５７において、通信装置２００２、２００３は、受信した平均入力伝送帯域値を基に算出した攻撃容疑パケットの伝送帯域制限調整値を含んだ伝送帯域制限調整指示を、全上流の通信装置、すなわち、通信装置２００２はその上流にある通信装置２００４に、通信装置２００３はその上流にある通信装置２００５及び２００６に送信する。このときの算出方法は、ゲート装置２００１のステップＳ３０４３と同様である。

【００４５】図１０の送帯域制限調整の算出の例を用いて説明する。通信装置２００２の１番目の１つ上流の通信装置２００４の平均入力伝送帯域値Ｂ(2, 1, 1)は４００ｋｂｐｓである。よって、（数２４）の右辺の分母は、全上流の通信装置からの平均入力伝送帯域値の合計を示していることより、Ｂ(2, 1, 1)と同値になる。また、通信装置２００２の伝送帯域制限調整値の初期値Ｓｓ’(1, 1)＝Ｓｓ’(1, 1, 1)であるため、ステップＳ３０４３より、Ｓｓ’(1, 1)は６４０ｋｂｐｓである。よって、通信装置２００２の１番目の１つ上流の通信装置２

００４の攻撃容疑トラヒックの伝送帯域制限調整値Ｓｓ’(2,1,1)は、Ｂ(2,1,1)＝４００ｋｂｐｓを分母４００ｋｂｐｓで除算し、伝送帯域制限調整値の初期値Ｓｓ’(1,1)＝６４０ｋｂｐｓを乗算した６４０ｋｂｐｓとなる。

【００４６】一方、通信装置２００３の１番目の１つ上流の通信装置２００５から通信装置２００３に入力される攻撃容疑トラヒックの平均入力伝送帯域値Ｂ(2,2,1)は０ｋｂｐｓ、２番目の１つ上流の通信装置２００６から通信装置２００３に入力される攻撃容疑トラヒックの平均入力伝送帯域値Ｂ(2,2,2)は１００ｋｂｐｓである。よって、（数２４）の右辺の分母は、全上流の通信装置からの平均入力伝送帯域値の合計を示していることより、Ｂ(2,2,1)＋Ｂ(2,2,2)＝１００ｋｂｐｓと算出される。また、通信装置２００３の伝送帯域制限調整値の初期値Ｓｓ’(1,2)＝Ｓｓ’(1,1,2)であるため、ステップＳ３０４３より、Ｓｓ’(1,2)は１６０ｋｂｐｓである。従って、通信装置２００５の攻撃容疑トラヒックの伝送帯域制限調整値Ｓｓ’(2,2,1)は、Ｂ(2,2,1)＝０ｋｂｐｓを分母１００ｋｂｐｓで除算し、伝送帯域制限調整値の初期値Ｓｓ’(1,2)＝１６０ｋｂｐｓを乗算した０ｋｂｐｓとなり、通信装置２００６の攻撃容疑トラヒックの伝送帯域制限調整値Ｓｓ’(2,2,2)は、Ｂ(2,2,2)＝１００ｋｂｐｓを分母１００ｋｂｐｓで除算し、伝送帯域制限調整値の初期値Ｓｓ’(1,2)＝１６０ｋｂｐｓを乗算した１６０ｋｂｐｓとなる。

【００４７】そして、図１１のステップ３０６３において、通信装置２００４～２００６は、通信装置２００２、２００３から伝送帯域制限調整指示を受信する。ステップＳ３０６４に進み、通信装置２００４～２００６は、容疑キュー２０２７の伝送帯域制限値を受信した伝送帯域制限指示に含まれる伝送帯域制限調整値に変更する。これにより、以後、図４に示す帯域制御モデルと図５に示すフィルタ２０２１の分類アルゴリズムに従って容疑シグネチャに合致する攻撃容疑パケットの伝送帯域は伝送帯域制限調整値に制限される。

【００４８】一方、ステップＳ３０４４において、ゲート装置２００１は、上記の伝送帯域制限調整から一定時間後、あるいは、受信する攻撃容疑パケットの伝送帯域が伝送帯域調整前と調整後である一定の割合変化した場合などのトリガを検出すると、再び伝送帯域調整を実行するステップＳ３０４１から伝送帯域制限調整値の調整を繰り返す。

【００４９】ところで、以上説明した動作は、以下に記述するアクティブネットワーク上で実行される。

【００５０】以下、図面を参照しこの発明の一実施形態を実行できるアクティブネットワークについて説明する。図１２は、本実施形態が前提とするネットワークの構成である。図１２に示すように、通信ネットワークは、複数の通信装置７００１によって接続されている。そして、通信装置７００１には１台または複数台のユーザのコンピュータ７０００を接続することができるようになっている。ユーザのコンピュータ７０００相互間で通信データのやりとりを行う際には、送信元のユーザのコンピュータ７０００が送信したパケットを通信ネットワーク上の各ノードに位置する通信装置７００１が順次転送することにより、そのパケットを宛先のユーザのコンピュータ７０００に届けるようにする。

【００５１】次に、通信装置の構成について説明する。図１３は、通信装置７００１の内部の構成を示すブロック図である。図１３に示すように、通信装置７００１には通信線７０２４ａ、７０２４ｂ、７０２４ｃ、７０２４ｄが接続されており、通信装置７００１はこれらの通信線を介して隣接する他の通信装置との間でパケットを交換することができるようになっている。また、通信装置７００１には、上記の各通信線７０２４ａ～７０２４ｄに対応したインタフェース部７０２３ａ～７０２３ｄと、パケットを転送する処理を行うための転送処理部７０２１と、パケットの転送の際の転送先の情報を記憶する転送先テーブル７０２２と、アクティブパケットに対する処理を行うためのアクティブネットワーク実行環境（ActiveNetwork Execution Environment）７０１０とが設けられている。なお、アクティブネットワーク実行環境７０１０は、内部に、アクティブコード（プログラム）を実行するためのコード実行部７０１１と、アクティブコードを記憶しておくためのコード記憶部７０１２とを備えている。なお、ここでアクティブコードとは、アクティブネットワークにおいてパケットに対する作用を行うコンピュータプログラムのコードである。

【００５２】ここで、図１３を参照しながら、この通信装置７００１の動作例の概要を説明する。隣接する他の通信装置から通信線７０２４ｄを介してパケットが到着すると、インタフェース部７０２３ｄがそのパケットを受信し転送処理部７０２１に渡す。転送処理部７０２１は、渡されたパケットのヘッダ部分に格納されている送信元（source）アドレスと宛先（destination）アドレスとを読み取り、さらにそれらのアドレスをキーとして転送先テーブル記憶部７０２２に記憶されている転送先テーブルを参照することによって、そのパケットにどう対処するかを決定する。

【００５３】パケットへの対処は大きく２通りに分けられる。そのパケットに対してアクティブコードを適用する場合と、そのパケットをそのまま他の通信装置に転送する場合とである。転送先テーブルを参照した結果、そのパケットに対してアクティブコードを適用すべきものである場合には、転送処理部７０２１は、そのパケットをアクティブネットワーク実行環境７０１０に渡す。アクティブネットワーク実行環境７０１０においては、コード実行部７０１１がそのパケットを受け取り、そのパケットに対して適用すべきアクティブコードをコード記

億部７０１２から読み出して実行する。なお、コード実行部７０１１は、アクティブコードを実行した結果、必要な場合には処理対象となったパケットを再び転送処理部７０２１に渡して他の通信装置に対して転送することもある。転送先テーブルを参照した結果、そのパケットにアクティブコードを適用せずそのまま他の転送装置に転送するべきものである場合には、転送処理部７０２１は、適切な転送先に対応したインタフェース部（７０２３ａや７０２３ｂや７０２３ｃなど）に渡し、そのインタフェース部が通信線（７０２４ａや７０２４ｂや７０２４ｃなど）を介してパケットを他の通信装置に転送する。

【００５４】なお、ここでは通信線７０２４ｄを介して他の通信装置からパケットが到着した場合を例として説明したが、他の通信線を介してパケットが到着した場合の処理も同様である。

【００５５】次に、通信装置７００１内の転送処理部７０２１がいかにしてパケットに対する処置（アクティブコードを適用するか、単純に他の通信装置に転送するか）を決定するかを具体的に説明する。

【００５６】本実施形態が基礎とするフレームワークでは、アクティブネットワーク実行環境はパケットの中において指定されているＩＰアドレスに基づいて起動される。ここで、全ての（グローバル）ＩＰアドレスの集合をＩと表わすものとする。また、送信元ＩＰアドレスがｓであり宛先ＩＰアドレスがｄであるようなパケットを（ｓ，ｄ）と表わすものとする。また、通信装置のアクティブネットワーク実行環境に格納されているすべてのアクティブコードはそれぞれ特定のユーザに属するものとし、ある特定のユーザの所有するＩＰアドレスの集合をＯと表わすものとする。

【００５７】本フレームワークでは、上記特定のユーザに属する個々のアクティブコードは、次に示す式による集合Ａで表されるパケットであって、かつ当該アクティブネットワーク実行環境を備えた通信装置（ノード）によって受信されたパケットに対してアクセスする権限を持つ。すなわち、

Ａ＝｛（ｓ，ｄ）∈［（Ｏ×Ｉ）∪（Ｉ×Ｏ）］｜ｓ≠ｄ｝

である。つまり、この式が意味するところの概略は、特定のユーザに属するアクティブコードは、当該ユーザが所有する全てのＩＰアドレスのいずれかを送信元または宛先のアドレスとするようなパケットに対してアクセス権を有するということである。

【００５８】当該ユーザに属するｎ個のアクティブコードがある通信装置（ノード）に格納されているとき、ｉ番目（１≦ｉ≦ｎ）のアクティブコードは、集合Ｃ（ｉ）（Ｃ（ｉ）⊆Ａ）に属するパケットをキャプチャーして処理することをアクティブネットワーク実行環境に対して予め要求しておく。つまり、当該ユーザに関して、アクティブネットワーク実行環境は、ｃ（１）Ｕｃ（２）Ｕ・・・・・Ｕｃ（ｎ）なる和集合の要素であるパケット（ｓ，ｄ）によって起動されるものであり、このようなパケットを「アクティブパケット」と呼ぶことができる。

【００５９】図１４は、図１３に示した転送先テーブル記憶部７０２２に記憶されている転送先テーブルの一例を示す概略図である。上記のフレームワークを実現するために必要な情報は、このような転送先テーブルに格納することが可能である。

【００６０】図１４に示すように、転送先テーブルは、タイプ（Type）と宛先アドレス（Destination）と送信元アドレス（Source）と転送先（Send to）の各項目を含んでいる。タイプの項目は、テーブルのエントリーのタイプを表わすものであり、「アクティブ（Active）」あるいは「通常（Regular）」のいずれかの値をとる。宛先アドレスおよび送信元アドレスの項目は、転送対象のパケットの宛先ＩＰアドレスおよび送信元ＩＰアドレスにそれぞれ対応するものである。転送先の項目はは、宛先アドレスと送信元アドレスの組み合せがマッチしたパケットに関して、適用すべきアクティブコードの識別情報あるいは転送先の通信装置のＩＰアドレスを表わすものである。

【００６１】タイプの値が「アクティブ」であるエントリーは、対象のパケットに適用するアクティブコードを指定するものであり、その転送先の項目にはアクティブコードを識別する情報が書かれている。タイプの値が「通常」であるエントリーは、対象のパケットの転送先の通信装置のアドレスを指定するものであり、その転送先の項目には転送先の通信装置のＩＰアドレスが書かれている。

【００６２】図１４に示す転送先テーブルの例において、第１のエントリーでは、タイプが「アクティブ」であり、宛先アドレスが「１．２．３．４」であり、送信元アドレスが「Ａｎｙ（何でもよい）」であり、転送先が「アクティブコードＡ」となっている。これは、送信元アドレスがいかなるアドレスであっても、宛先アドレスが「１．２．３．４」にマッチする場合には、該当するパケットをトリガーとしてアクティブネットワーク実行環境が起動され、アクティブコードＡが実行されることを表わしている。また、第２のエントリーでは、タイプが「アクティブ」であり、宛先アドレスが「１０．５０．０．０」であり、送信元アドレスが「１１．１２．１３．１４」であり、転送先が「アクティブコードＢ」となっている。これは、宛先アドレスと送信元アドレスの両方がそれぞれ上記の値にマッチした場合には、該当するパケットをトリガーとしてアクティブネットワーク実行環境が起動され、アクティブコードＢが実行されることを表わしている。また、第３のエントリーでは、タイプが「アクティブ」であり、宛先アドレスが「Ａｎｙ

33

（何でもよい）」であり、送信元アドレスが「１５７．２．３．０」であり、転送先が「アクティブコードＣ」となっている。これは、宛先アドレスがいかなるアドレスであっても、送信元アドレスが「１５７．２．３．０」にマッチする場合には該当するパケットをトリガーとしてアクティブネットワーク実行環境が起動され、アクティブコードＣが実行されることを表している。

【００６３】なお、図１４に示すように、転送先テーブルにおいては、タイプが「アクティブ」であるエントリーのほうが、タイプが「通常」であるエントリーよりも上に存在している。そして、タイプが「アクティブ」であるエントリーのほうが、タイプが「通常」であるエントリーよりも優先的に適用される。また、各エントリーは、通信装置へ到着したパケットのみに対して適用され、転送のために送出されるパケットに対しては適用されない。

【００６４】以上説明した通信装置の構成をまとめる。図１３に示したインタフェース部は、通信線毎に設けられており、当該通信線から到着するパケットを受信するとともに当該通信線に対してパケットを送出する処理を行う。また、転送先テーブル記憶部は、パケットの送信元アドレスまたは宛先アドレスまたはそれら両方のアドレスのパターンと、該パターンに対応するプログラム（アクティブコード）の情報あるいは該パターンに対応する転送先アドレスの情報とが登録された転送先テーブルを記憶する。また、アクティブネットワーク実行環境は、前記プログラムを予め記憶しているとともに、このプログラムを実行する。また、転送処理部は、通信線から到着した受信パケットを前記インタフェース部から渡された際に、当該受信パケットの送信元アドレスまたは宛先アドレスに基づいて前記転送先テーブルを参照し、前記転送先テーブルに当該受信パケットのアドレスのパターンに対応する転送先アドレスの情報が登録されていた場合には当該受信パケットを所定の転送先アドレスに向けて送出するように当該転送先アドレスに対応したインタフェース部に渡すとともに、前記転送先テーブルに当該受信パケットのアドレスのパターンに対応するプログラムの情報が登録されていた場合には前記アクティブネットワーク実行環境部において当該プログラムを起動させるとともに当該プログラムに当該受信パケットを渡す。

【００６５】次に、本実施形態におけるアクティブコードのセキュリティに関するモデルについて説明する。このセキュリティのモデルは、各々のアクティブコードが、アクティブコードの所有者に関わるパケットのみに対して作用することを保証するためのものである。そのために、このセキュリティのモデルは、公開鍵のインフラストラクチャの存在を前提として、それを利用することとする。

【００６６】図１５は、上記のセキュリティモデルとそ

34

のモデルにおける処理の手順を示す概略図である。図１５において、符号７０５１はユーザＡのユーザ端末装置、７０６１は認証局（Certification Authority）装置である。この認証局の機能は、公の機関によって提供されるものであっても良いし、あるいはＩＳＰ（Internet Service Provider,インターネット接続サービス提供者）などによって提供されるものであっても良い。なお、図１５に示す例では、ユーザ端末装置７０５１のＩＰアドレスは「１．２．３．４」である。以下では、ユーザＡが、アクティブコードＡを通信装置７００１に登録するための処理の手順を説明する。なお、以下において、ユーザＡはアクティブコードＡの開発者であっても良いが、その必然性はなく、他の開発者が開発したアクティブコードＡをユーザＡが入手し、それを通信装置７００１に登録するものでも良い。

【００６７】まず（１）で示すように、ユーザＡのユーザ端末装置７０５１は、周知技術を用いて鍵のペアすなわち公開鍵と秘密鍵とを生成する。そして（２）で示すように、ユーザ端末装置７０５１は、上で生成された公開鍵を認証局装置７０６１に登録する。このとき、認証局装置７０６１は、ユーザ端末装置７０５１のＩＰアドレスを検証する。この検証が正しく行なわれると、公開鍵そのものと、ユーザＡを識別するための情報と、ユーザ端末装置７０５１のＩＰアドレス「１．２．３．４」が認証局装置７０６１に記憶される。

【００６８】次に（３）で示すように、ユーザ端末装置７０５１は、上で生成された秘密鍵を用いてアクティブコードＡに電子署名する処理を行う。そして（４）で示すように、ユーザ端末装置７０５１は、秘密鍵で署名されたアクティブコードＡを通信装置７００１に登録する処理を行う。

【００６９】これを受けて通信装置７００１は、（５）で示すように、アクティブコードＡの登録を行ったユーザＡの電子証明書を認証局装置７０６１から取得する。この電子証明書には、ユーザＡを識別する情報と、そのＩＰアドレス「１．２．３．４」と、上の（２）において登録された公開鍵そのものとが含まれている。そして（６）で示すように、通信装置７００１は、上記の電子証明書から取り出したユーザＡの公開鍵を用いて、上の（４）において登録されたアクティブコードＡの電子署名を検証する。そして、これが正しく検証された場合には、通信装置７００１は、アクティブコードＡをアクティブネットワーク実行環境に導入する処理を行う。また、これに応じて、転送先テーブルに必要なエントリーが追加される。

【００７０】なお、この（１）および（２）の処理が行われて一旦ユーザＡの公開鍵が認証局装置７０６１に登録されると、ユーザ端末装置７０５１はその公開鍵に対応する秘密鍵を用いてアクティブモジュールをいくつでも通信装置７００１に登録することも可能である。

35

【００７１】つまり、通信装置７００１は登録部（図示せず）を備えており、この登録部は、ユーザの端末装置から当該ユーザの秘密鍵で電子署名されたプログラムを受信し、当該ユーザの電子証明書を認証局装置から受信し、受信した電子証明書に含まれる当該ユーザの公開鍵を用いて前記電子署名されたプログラムの検証を行い、この検証が成功した場合には当該プログラムに対応するアドレスのパターンと当該プログラムの情報とを前記転送先テーブルに登録し、この検証が失敗した場合には当該プログラムの情報の前記転送先テーブルへの登録は行わないようにするものである。

【００７２】なお、上で説明した通信装置へのアクティブコードの登録の手順が有効に機能するためには、次の２点が前提となる。第１の前提として、ユーザがどの通信装置（ノード）にアクティブコードを登録すれば良いかは事前にわかっている。あるいは、どの通信装置（ノード）にアクティブコードを登録すればよいかがわかるためのディレクトリサービスが提供されている。第２の前提として、通信装置（ノード）は、目的の認証局の公開鍵を事前にオフラインで取得しているか、他の認証局から取得するか、あるいは他の何らかの手段で取得できる。

【００７３】次に、矛盾の解消のための制御について説明する。ある通信装置（ノード）において、ｎ個のアクティブコードが登録されており、ｉ番目（$1 \leqq i \leqq n$）とｊ番目（$1 \leqq j \leqq n$）のアクティブコードが、それぞれ集合Ｃ（ｉ）（Ｃ（ｉ）⊆Ａ）と集合Ｃ（ｊ）（Ｃ（ｊ）⊆Ａ）に属するパケットに対するものであると定義されているとき、集合（ｃ（ｉ）∩ｃ（ｊ））が空集合ではないようなｉおよびｊの組み合せ（但しｉ≠ｊ）が存在する場合があり得る。つまり、あるパケットがｉ番目のアクティブコードにもｊ番目のアクティブコードにも適用されるような定義が行われている場合である。このような矛盾は、次の２通りのシナリオのいずれかによって解消することとする。

【００７４】第１の矛盾の解消のシナリオは、パケット（ｓ，ｄ）に関して、

（ｓ∈Ｏ（ｋ）∧ｄ∈Ｏ（ｌ））∧（ｋ≠ｌ）

であるために、

（ｓ，ｄ）∈ｃ（ｉ）∩ｃ（ｊ）

となる場合に関するものである。但し、Ｏ（ｋ）およびＯ（ｌ）は、それぞれユーザｋおよびｌによって所有されるＩＰアドレスの集合である。つまり、あるパケットに関して、送信元のユーザ用のアクティブコードと宛先のユーザ用のアクティブコードとの両方が通信装置に登録されており、そのような通信装置にこのパケット（ｓ，ｄ）が到着した場合である。このような場合には、宛先のユーザのアクティブコードを優先的に適用することが望ましいと考えられる。

【００７５】つまり、転送先テーブルに登録されている

36

パターンに、送信元アドレスのみが指定されていて宛先アドレスが何でもよいとされている第１のエントリーと、宛先アドレスのみが指定されていて送信元アドレスが何でもよいとされている第２のエントリーとが含まれており、受信パケットがこれら第１のエントリーと第２のエントリーとの両方にマッチしたときには、第１のエントリーよりも第２のエントリーを優先させて、当該第２のエントリーのパターンに対応するプログラムを起動するようにする。

【００７６】このように、送信元のユーザのアクティブコードよりも宛先のユーザのアクティブコードを優先させることは、アクティブネットワークの機能を用いてＤＤｏＳ（分散型ＤｏＳ，Distributed Denial of Service）攻撃を防御するメカニズムを構築する場合に特に重要となる。そのようにすることによって、宛先のユーザつまり被攻撃者となり得る者のアクティブコードが、攻撃者となる可能性があるもののアクティブコードよりも優先されるためである。

【００７７】第２の矛盾の解消のシナリオは、あるパケット（ｓ，ｄ）に関して適用されるべき２つ以上のアクティブコードが同一のユーザによって登録されている場合に関するものである。このような場合には、該当するアクティブコードのうちの最も古く登録されたものが、他のものよりも優先的に適用されるようにすることが望ましいと考えられる。こうすることにより、ユーザが新しいアクティブコードを登録しようとする際には、新しいアクティブコードを有効にするために事前に古いアクティブコードを削除することが保証されるからである。

【００７８】次に、これまでに述べたようなアクティブネットワークのノードとして機能する通信装置のインプリメンテーションの例について説明する。図１６は、Ｌｉｎｕｘ上のＪａｖａ（登録商標）仮想マシン（ＪＶＭ）を用いてアクティブパケットの処理を行う通信装置を実現した場合の概略図である。

【００７９】図１６に示す例では、専用のＩＰスタックを処理（process）の一部として構築している。これによって、図１４に示したような転送先テーブルを実現し、実行環境（アクティブネットワーク実行環境）からこの転送先テーブルにエントリーの追加や削除を行えるようにしている。また、これに伴い、カーネル（kernel）内のＩＰスタックは不要となるため、カーネルにおけるルーティングを不活性化している。そして、到着パケットのコピーがデータリンク部分から作成され、そのパケットがライブラリｌｉｂｐｃａｐを通してＪａｖａ（登録商標）仮想マシンで補足できるようにしている。

【００８０】処理の一部として構築した専用のＩＰスタックは、アクティブパケット、つまり転送先テーブル上での所定の定義にマッチするＩＰアドレス（宛先ＩＰアドレス、送信元ＩＰアドレス、あるいはそれらの組み合せ）を有するパケットは、実行環境上で起動されるアク

ティブコードに対して渡される。一方、アクティブパケット以外の通常のパケットは、カーネルにおけるＩＰスタックと同様の方法で隣接する通信装置等へ向けた転送が行われる。アクティブパケットであれ通常パケットであれ、この通信装置から送出されるすべてのパケットは、ライブラリｌｉｂｎｅｔを通して送出される。こうすることにより、各々処理されたパケットのヘッダに記録された送信元アドレスは、元々の送信元アドレスのままの状態で、ネットワークに送出されることとなる。

【００８１】また、標準のＪａｖａ（登録商標）のＡＰＩ（アプリケーションプログラムインタフェース）である「java.security」を用いることによってセキュリティモデルをインプリメンテーションすることが可能である。この標準ＡＰＩは、セキュリティモデルを構築するために必要な機能のほとんどを提供している。また、証明書のための形式としては「Ｘ．５０９」証明書形式を用いることが可能であり、アクティブコードの所有者のＩＰアドレスを「Ｘ．５０９」の識別名（ＤＮ，distinguished name）の一部に含めることにより、本実施形態のセキュリティモデルを実現することができる。

【００８２】なお、言うまでもなく、上記インプリメンテーションではコンピュータシステムを用いることによってアクティブネットワーク実行環境を備えた通信装置を構築している。そして、上述した一連の処理、すなわち到着パケットの複製の作成とその捕捉や、転送先テーブルを参照しながらのアクティブパケットおよび通常パケットの転送の処理や、アクティブネットワーク実行環境上でのアクティブコードの起動とその処理の実行や、処理されたパケットのネットワークへの送出などの各処理の過程は、プログラムの形式でコンピュータ読み取り可能な記録媒体に記憶されており、このプログラムをコンピュータが読み出して実行することによって、上記処理が行われる。

【００８３】なお、上述した各コンピュータプログラムは、コンピュータ読取可能な記録媒体に記録されており、通信装置等に搭載されたＣＰＵ（中央処理装置）がこの記録媒体からコンピュータプログラムを読み取って、攻撃防御あるいはサービスモジュール提供等のための各処理を実行する。また、「コンピュータ読み取り可能な記録媒体」とは、磁気ディスク、光磁気ディスク、ＲＯＭ、ＣＤ－ＲＯＭ等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムが送信された場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリ（ＲＡＭ）のように、一定時間プログラムを保持しているものも含むものとする。

【００８４】また、上記プログラムは、このプログラムを記憶装置等に格納したコンピュータシステムから、伝送媒体を介して、あるいは、伝送媒体中の伝送波により他のコンピュータシステムに伝送されても良い。ここで、プログラムを伝送する「伝送媒体」は、インターネット等のネットワーク（通信網）や電話回線等の通信回線（通信線）のように情報を伝送する機能を有する媒体のことをいう。

【００８５】また、上記プログラムは、前述した機能の一部を実現するためのものであっても良い。さらに、前述した機能をコンピュータシステムに既に記録されているプログラムとの組み合わせで実現できるもの、いわゆる差分ファイル（差分プログラム）であっても良い。

【００８６】また、下流のゲート装置または通信装置から上流の通信装置へのデータの送信は、アクティブネットワークの使用に限定するものではなく、任意の通信プロトコルの使用が可能である。

【００８７】また、ゲート装置及び通信装置はゲートウェイやルータに限られるものではなく、ブリッジ、イーサネット（登録商標）、インタフェース変換装置など、ＩＰアドレスを持つ任意の通信ノードであっても良い。

【００８８】以上、図面を参照してこの発明の実施形態を詳述してきたが、具体的な構成はこれらの実施形態に限られるものではなく、この発明の要旨を逸脱しない範囲の設計等も含まれる。

【００８９】

【発明の効果】以上説明したように、ＤＤｏＳ攻撃の被攻撃者の通信装置がＤＤｏＳ攻撃の攻撃の容疑トラヒックを検出すると、初期の伝送帯域制御により、その上流の各通信装置で攻撃容疑トラヒックの伝送帯域を制限することが可能になるため、早期にネットワークの輻輳を改善することが可能となり、ＤＤｏＳ被攻撃者のサービスの停止を抑止することが可能になるとともに、正規利用者からの通信パケットの割合を増加させることが可能になる。

【００９０】また、初期の伝送帯域制御による攻撃容疑パケットの帯域制限後は、各通信装置の攻撃容疑パケットの入力伝送帯域に応じて伝送帯域制限値が調整することが可能になるため、伝送帯域をネットワーク上の各通信装置に有効に分配することが可能となり、攻撃容疑パケットとして分類された正規パケットの伝送帯域を増加させ、正規ユーザのサービス性の低下を段階的に改善することが可能になる。

【図面の簡単な説明】

【図１】　本発明の実施の形態を適用できるネットワークの構成図である。

【図２】　同実施の形態による攻撃容疑検出条件の設定の例である。

【図３】　同実施の形態による不正トラヒック検出条件の設定の例である。

【図４】　同実施の形態によるゲート装置２００１及び通信装置２００２～２００６が備える帯域制御モデルで

ある。

【図５】　同実施の形態によるフィルタ２０２１における分類アルゴリズムである。

【図６】　同実施の形態によるゲート装置２００１の攻撃容疑パケット検出時の動作を示すフローチャートである。

【図７】　同実施の形態による図１の構成における伝送帯域制限値の算出の例である。

【図８】　同実施の形態による通信装置２００２、２００３の伝送帯域制限指示受信時の動作を示すフローチャートである。

【図９】　同実施の形態によるゲート装置２００１及び通信装置２００２～２００６の不正トラヒック検出時の動作を示すフローチャートである。

【図１０】　同実施の形態による図１の構成における伝送帯域制限調整値の算出の例である。

【図１１】　同実施の形態によるゲート装置２００１及び通信装置２００２～２００６の伝送帯域制限値の調整の動作を示すフローチャートである。

【図１２】　同実施の形態を実行できるアクティブネットワークが前提とするネットワークの構成である。

【図１３】　同実施の形態を実行できるアクティブネットワークによる通信装置内部の構成を示すブロック図である。

【図１４】　同実施の形態を実行できるアクティブネットワークによる転送先テーブル記憶部に記憶されている転送先テーブルの一例を示す概略図である。

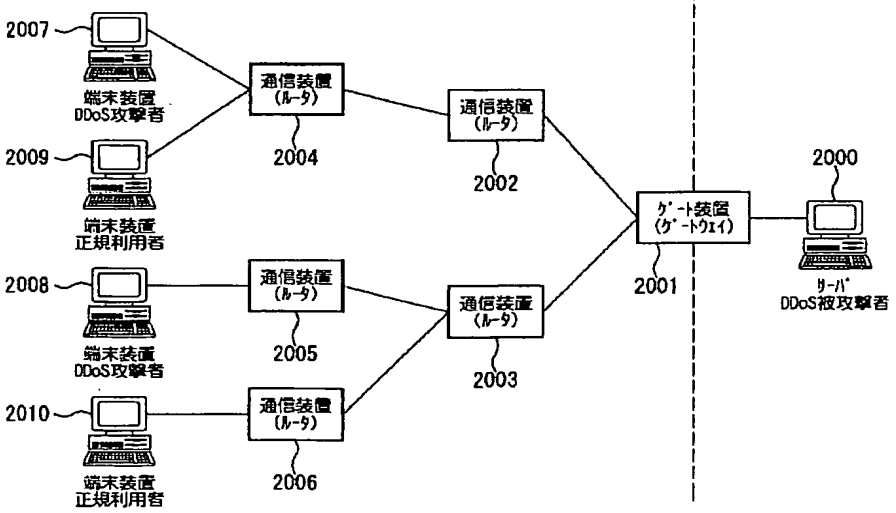
【図１５】　同実施の形態を実行できるアクティブネットワークによるセキュリティモデルとそのモデルにおける処理の手順を示す概略図である。

【図１６】　同実施の形態を実行できるアクティブネットワークの通信装置をＬｉｎｕｘ上のＪａｖａ（登録商標）仮想マシン（ＪＶＭ）を用いてアクティブパケットの処理を行うように実現した場合の概略図である。

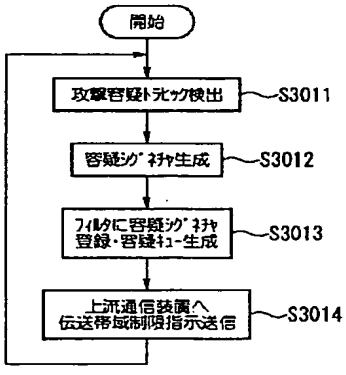
【符号の説明】

２０００…サーバ
２００１…ゲート装置
２００２～２００６…通信装置
２００７～２０１０…端末装置
２０２１…フィルタ
２０２２…正規クラス
２０２３…正規キュー
２０２４…不正クラス
２０２５…不正キュー
２０２６…容疑クラス
２０２７…容疑キュー
７０００…ユーザのコンピュータ
７００１…通信装置
７０１０…アクティブネットワーク実行環境
７０１１…コード実行部
７０１２…コード記憶部
７０２１…転送処理部
７０２２…転送先テーブル記憶部
７０２３ａ、７０２３ｂ…インタフェース部
７０２４ａ、７０２４ｂ…通信線
７０５１…ユーザ端末装置
７０６１…認証局装置

【図１】



【図６】



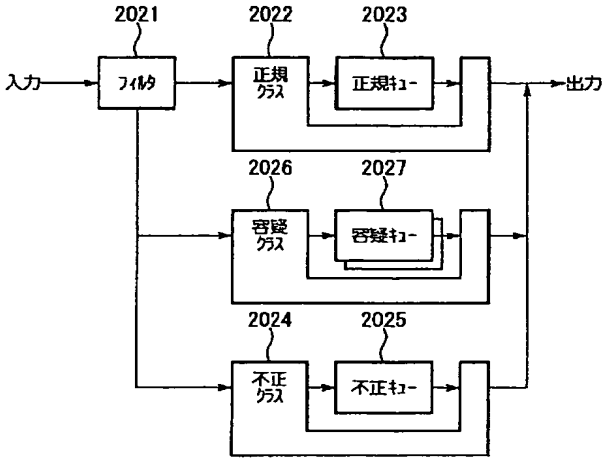
【図２】

番号	検出属性	検出閾値	検出間隔
1	{Dst=192.168.1.1/32,Protocol=TCP,Port=80}	500 kbps	10 秒
2	{Dst=192.168.1.2/32,Protocol=UDP}	300 kbps	10 秒
3	{Dst=192.168.1.0/24}	1 Mbps	20 秒

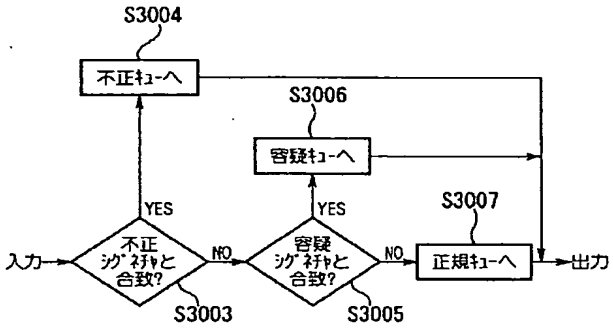
【図３】

番号	不正トラヒック条件
1	T1 Kbps 以上のパケットが S1 秒以上連続送信されている
2	T2 Kbps 以上の ICMP/Echo Reply パケットが S2 秒以上連続送信されている
3	T3 Kbps 以上のフラグメントパケットが S3 秒以上連続送信されている

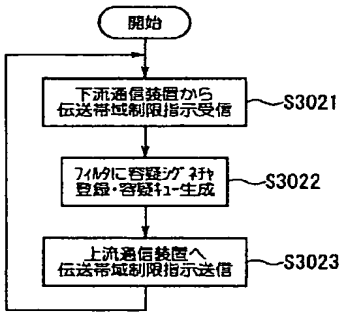
【図４】



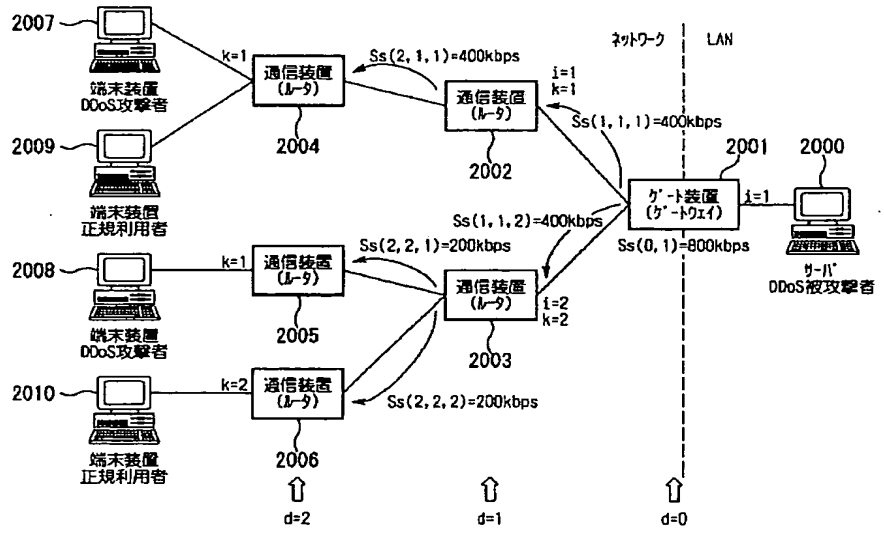
【図５】



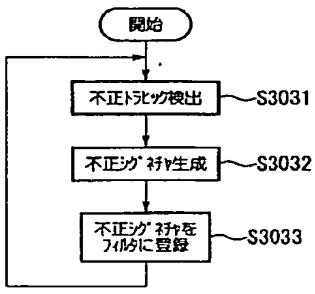
【図８】



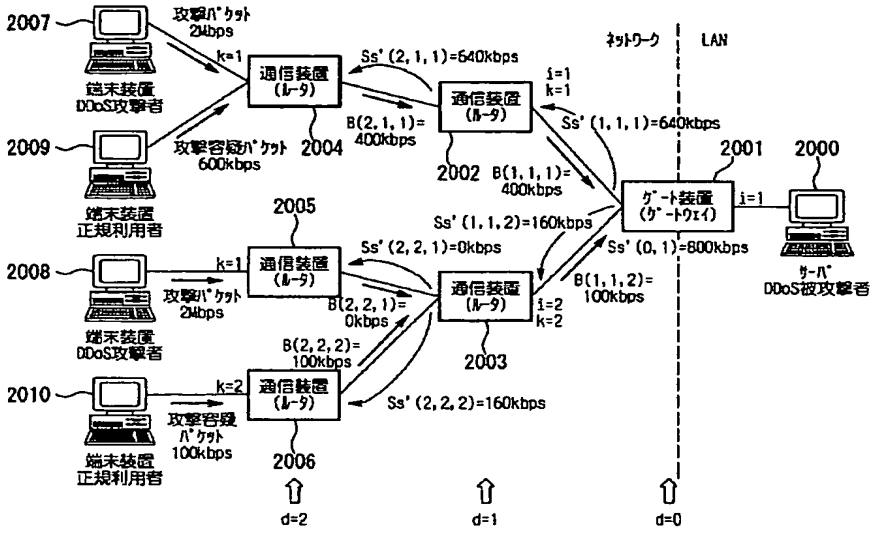
【図７】



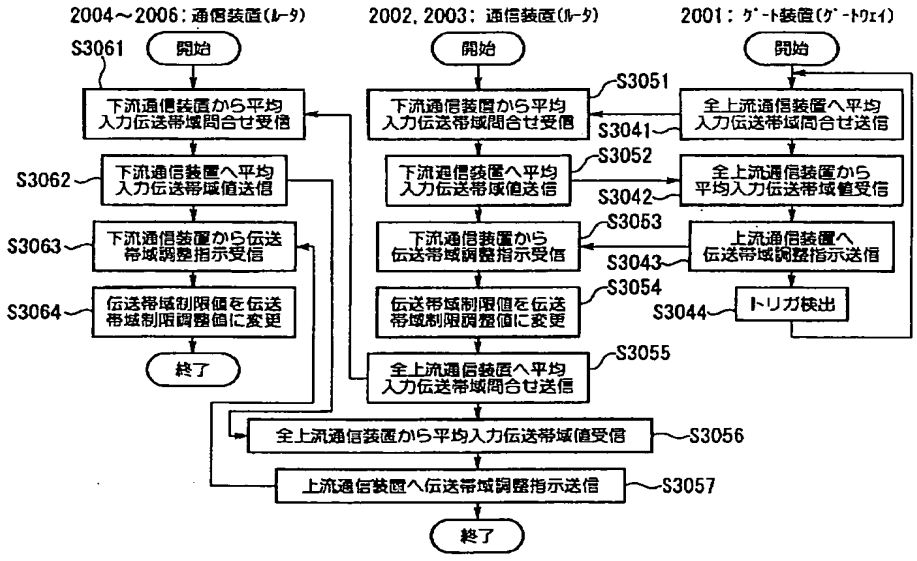
【図９】



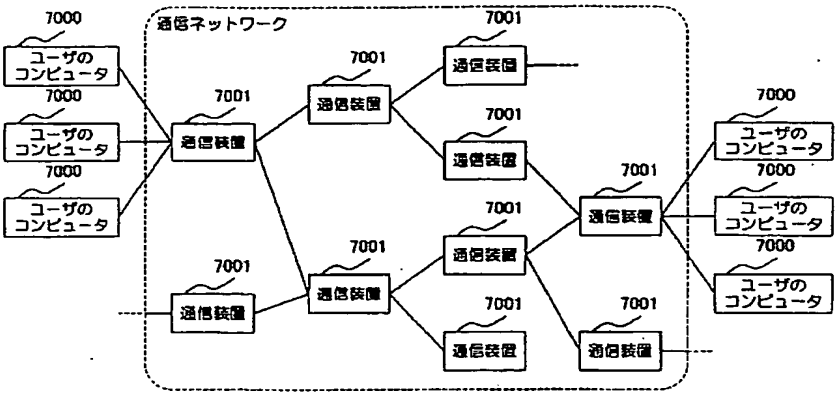
【図１０】


2007
攻撃ﾊﾟｹｯﾄ
2Mbps
k=1
通信装置
(ﾙｰﾀ)
Ss'(2,1,1)=640kbps
端末装置
DDoS攻撃者
2009
攻撃容疑ﾊﾟｹｯﾄ
600kbps
2004
B(2,1,1)=
400kbps
通信装置
(ﾙｰﾀ)
i=1
k=1
Ss'(1,1,1)=640kbps
ﾈｯﾄﾜｰｸ
LAN
2001
2000
2002
B(1,1,1)=
400kbps
ｹﾞｰﾄ装置
(ｹﾞｰﾄｳｪｲ)
i=1
端末装置
正規利用者
2005
Ss'(1,1,2)=160kbps
Ss'(0,1)=800kbps
ｻｰﾊﾞ
DDoS被攻撃者
2008
k=1
通信装置
(ﾙｰﾀ)
Ss'(2,2,1)=0kbps
攻撃ﾊﾟｹｯﾄ
2Mbps
B(2,2,1)=
0kbps
通信装置
(ﾙｰﾀ)
i=2
k=2
B(1,1,2)=
100kbps
端末装置
DDoS攻撃者
B(2,2,2)=
100kbps
2003
2010
k=2
通信装置
(ﾙｰﾀ)
Ss'(2,2,2)=160kbps
攻撃容疑
ﾊﾟｹｯﾄ
100kbps
端末装置
正規利用者
2006
d=2
d=1
d=0

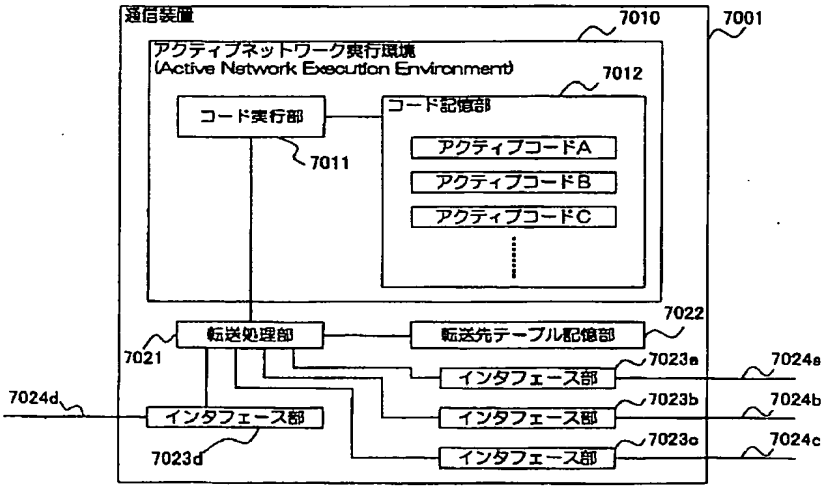
【図１１】


2004～2006：通信装置(ﾙｰﾀ)
2002, 2003：通信装置(ﾙｰﾀ)
2001：ｹﾞｰﾄ装置(ｹﾞｰﾄｳｪｲ)
開始
S3061
下流通信装置から平均
入力伝送帯域問合せ受信
S3062
下流通信装置へ平均
入力伝送帯域値送信
S3063
下流通信装置から伝送
帯域調整指示受信
S3064
伝送帯域制限値を伝送
帯域制限調整値に変更
終了
S3051
S3041
全上流通信装置へ平均
入力伝送帯域問合せ送信
S3052
S3042
全上流通信装置から
平均入力伝送帯域値受信
S3053
S3043
上流通信装置へ
伝送帯域調整指示送信
S3054
S3044
トリガ検出
S3055
全上流通信装置へ平均
入力伝送帯域問合せ送信
S3056
全上流通信装置から平均入力伝送帯域値受信
S3057
上流通信装置へ伝送帯域調整指示送信

【図１２】



【図１３】

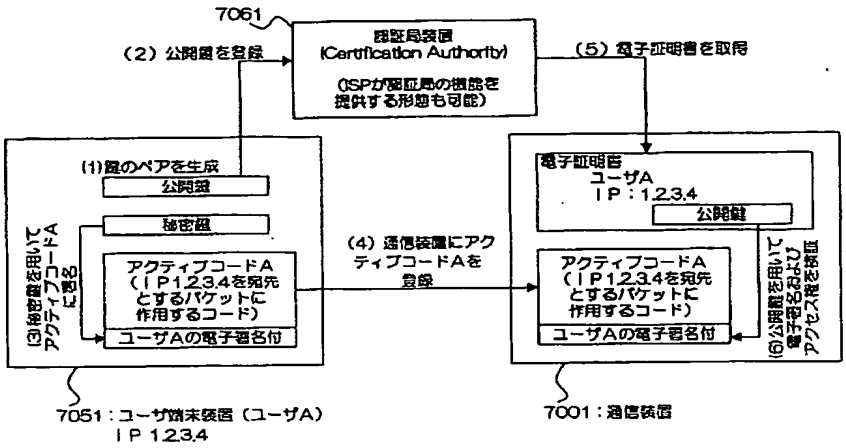


【図１４】

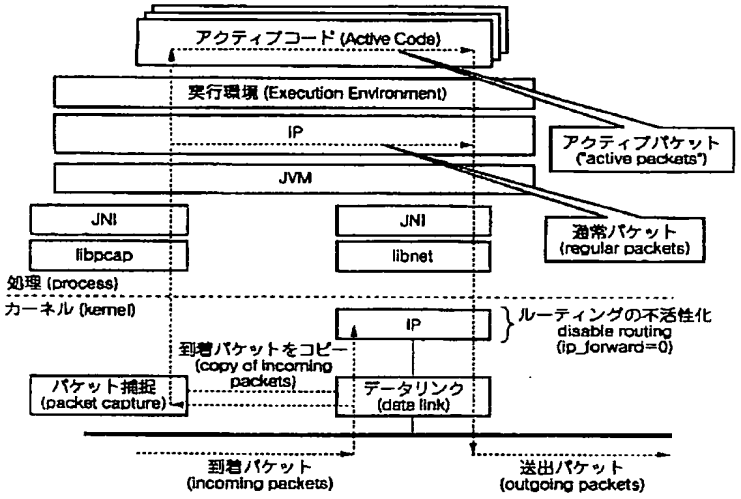
転送先テーブル

タイプ (Type)	宛先アドレス (Destination)	送信元アドレス (Source)	転送先 (Send to)
アクティブ (Active)	1.2.3.4	Any	アクティブコードA
アクティブ	10.50.0.0	11.12.13.14	アクティブコードB
アクティブ	Any	157.2.3.0	アクティブコードC
通常 (Regular)	1.2.0.0	N/A	29.15.20.1
通常	11.20.0.0	N/A	109.1.1.10
通常	199.1.1.0	N/A	120.0.0.1
⋮	⋮	⋮	⋮

【図１５】



【図１６】



フロントページの続き

(72)発明者　冨士　仁
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

Ｆターム(参考)　5K030 GA13 GA15 HA08 HB08 HB14 KA06 KX24 KX30 LC15 MD08
5K033 AA05 AA08 CB06 CB08 DA15 DB19 EA07